Supreme Court, U.S.
FILED
JUN 25 2004
OFFICE OF THE CLERK

(3)

No. 03-1579

IN THE

Supreme Court of the United States

RECORDING INDUSTRY ASSOCIATION OF AMERICA, INC.,

Petitioner,

v.

VERIZON INTERNET SERVICES, INC.,

Respondent.

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT

BRIEF IN OPPOSITION

ANDREW G. MCBRIDE
KATHRYN COMERFORD TODD
BRUCE G. JOSEPH
KARYN K. ABLIN
DINEEN PASHOUKOS WASYLIK
WILEY REIN & FIELDING LLP
1776 K Street NW
Washington, D.C. 20006
(202) 719-7000

JOHN THORNE*
SARAH B. DEUTSCH
THOMAS M. DAILEY
LEONARD CHARLES SUCHYTA
VERIZON COMMUNICATIONS INC.
1515 N. Courthouse Road
Fifth Floor
Arlington, Va. 22201
(703) 351-3900

Attorneys for Respondent

* *Counsel of Record*

188140

COUNSEL PRESS
(800) 274-3321 • (800) 359-6859

COUNTER STATEMENT OF QUESTIONS PRESENTED

1. Whether the D.C. Circuit, applying well-established canons of statutory construction, correctly concluded that the text, structure, and legislative history of the novel subpoena provision of the Digital Millennium Copyright Act, 17 U.S.C. § 512(h), all demonstrate that that provision applies only to circumstances in which potentially infringing material is stored on the Internet service provider's system or network.

2. Whether Petitioner's expansive interpretation and use of the novel subpoena provision contained in the Digital Millennium Copyright Act, 17 U.S.C. § 512(h), is precluded by the First Amendment to the United States Constitution.

3. Whether the issuance and enforcement of binding judicial process pursuant to 17 U.S.C. § 512(h), outside the context of a "case or controversy," violates Article III of the United States Constitution and fundamental principles of the constitutionally mandated separation of powers.

PARTIES TO THE PROCEEDING

Petitioner Recording Industry Association of America, Inc. was the appellee below. Respondent Verizon Internet Services Inc. was the appellant. The United States intervened pursuant to 28 U.S.C. § 2403 solely to defend the constitutionality of the subpoena provision of the Digital Millennium Copyright Act.

RULE 29.6 DISCLOSURE

Respondent is a wholly owned subsidiary of Bell Atlantic Entertainment and Information Services Group, Inc. Bell Atlantic Entertainment and Information Services Group, Inc. is a wholly owned subsidiary of Bell Atlantic Investment Development Corporation, which is a wholly owned subsidiary of Verizon Investments Inc. Verizon Investments Inc. is a wholly owned subsidiary of Verizon Communications Inc., a publicly held corporation. Verizon Communications Inc. does not have a parent company, and no publicly held company has a ten-percent or greater interest in it.

TABLE OF CONTENTS

	Page
Counter Statement of Questions Presented	i
Parties to the Proceeding	ii
Rule 29.6 Disclosure	ii
Table of Contents	iii
Table of Cited Authorities	vi
Table of Appendices	xii
Jurisdiction	1
Constitutional and Statutory Provisions Involved	1
Summary of Reasons for Denying the Petition	2
Statement of the Case	3
A. Legal and Factual Background	3
1. The Statutory Framework and Legislative Purpose of the DMCA	3
2. The Two Subpoenas at Issue in These Proceedings	9
B. The Proceedings Below	10
1. The District Court's Decisions	10
2. The Court of Appeals' Reversal of the District Court	11

Contents

Page

Reasons for Denying the Petition 14

I. The Petition Meets None Of The Established Justifications For Intervention By This Court. 14

A. There Is No Split of Authority on the Narrow Statutory Issue Resolved by the D.C. Circuit. 14

B. No Extraordinary Circumstances Justify Review. 15

C. RIAA's Policy Arguments Regarding New Technologies and Requests To Expand Copyright Protections Are Properly Addressed to Congress, Not to this Court. 16

II. The Court Of Appeals Correctly Applied Settled Canons Of Statutory Construction. 19

A. The Text, Structure, History, and Purpose of Section 512 Compel the Result Reached by the D.C. Circuit. 19

1. The Text and Structure of Section 512 Compel the Conclusion That Section 512(h) Applies Only to Material Stored on a Service Provider's System or Network. 19

Contents

Page

2. The Legislative History and Purpose of the Statute Further Confirm That Section 512(h) Does Not Apply to the Conduit Context. 24

B. The D.C. Circuit's Reading of the Statute Avoids Serious First Amendment Concerns. 25

C. The Existence of a Substantial Alternative Ground for Affirming the Judgment Below Militates Against Granting the Petition. 27

Conclusion 30

TABLE OF CITED AUTHORITIES

Page

CASES

Bennett v. Spear,
520 U.S. 154 (1997) 28

Blount v. Rizzi,
400 U.S. 410 (1971) 26

Buckley v. Valeo,
424 U.S. 1 (1976) 30

Christensen v. Harris County,
529 U.S. 576 (2000) 25

Columbia Insurance Co. v. Seescandy.com,
185 F.R.D. 573 (N.D. Cal. 1999) 26

E. Microwave, Inc. v. Doubleday Sports,
691 F.2d 125 (2d Cir. 1982) 4

Eldred v. Ashcroft,
537 U.S. 186 (2003) 18

Estate of Joseph Leder v. Commissioner of Internal Revenue,
893 F.2d 237 (10th Cir. 1989) 21

FDA v. Brown & Williamson Tobacco Corp.,
529 U.S. 120 (2000) 21

Freedman v. Maryland,
380 U.S. 51 (1965) 26

Cited Authorities

	Page
Gordon v. United States, 117 U.S. Appx. 697 (1864)	28
Hayburn's Case, 2 U.S. (2 Dall.) 408 (1792)	28
Hoffmann-La Roche, Inc. v. Sperling, 493 U.S. 165 (1989)	1, 28
In re Subpoena to North Carolina State University, No. 1:03mc139 (M.D.N.C.)	14
In re Subpoena to University of North Carolina, No. 1:03mc138 (M.D.N.C.)	14
Marbury v. Madison, 5 U.S. (1 Cranch) 137 (1803)	1, 28
McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995)	25
Muskrat v. United States, 219 U.S. 346 (1911)	28
Overseas Education Association v. FLRA, 824 F.2d 61 (D.C. Cir. 1987)	21
Philadelphia Newspapers, Inc. v. Hepps, 475 U.S. 767 (1986)	26
RIAA v. Charter Communications, Inc., No. 03-3802 (8th Cir.)	14

Cited Authorities

Page

S&E Contractors, Inc. v. United States,
406 U.S. 1 (1972) 24

Sony Corp. of Am. v. Universal City Studios, Inc.,
464 U.S. 417 (1984) 13, 18

Stanley v. Georgia,
394 U.S. 557 (1969) 27

Steel Co. v. Citizens for a Better Environment,
523 U.S. 83 (1998) 1, 27

United States v. Ferreira,
54 U.S. (13 How.) 40 (1851) 28

United States v. Mead Corp.,
533 U.S. 218 (2001) 25

United States v. Morton Salt Co.,
338 U.S. 632 (1950) 1, 28, 29

United States Catholic Conference v. Abortion Rights Mobilization, Inc.,
487 U.S. 72 (1988) 1, 28, 29

United States Railroad Retirement Board v. Fritz,
449 U.S. 166 (1980) 24

Williams v. Taylor,
529 U.S. 362 (2000) 22

Yale Todd's Case, printed at 54 U.S.
(13 How.) 52 (1851) 28

Cited Authorities

Page

CONSTITUTION AND STATUTES

U.S. Const. amend. I 1

U.S. Const. art. III ..... *passim*

17 U.S.C. § 512 1

17 U.S.C. § 512(a) ..... *passim*

17 U.S.C. § 512(b) ..... *passim*

17 U.S.C. § 512(c) ..... *passim*

17 U.S.C. § 512(d) ..... *passim*

17 U.S.C. § 512(f) 6, 20, 23, 27

17 U.S.C. § 512(g) ..... *passim*

17 U.S.C. § 512(h) ..... *passim*

17 U.S.C. § 512(i) 5, 22

17 U.S.C. § 512(j) 5, 21, 22

17 U.S.C. § 512(k) 12

17 U.S.C. § 512(m) 9

17 U.S.C. § 512(n) 6

17 U.S.C. § 1201 ..... 1, 3

17 U.S.C. § 1202 ..... 1, 3

Cited Authorities

	Page
17 U.S.C. § 1203	1, 3
17 U.S.C. § 1204	1, 3
17 U.S.C. § 1205	1, 9
28 U.S.C. § 956	30
28 U.S.C. § 2403	ii

LEGISLATIVE MATERIALS

H.R. Rep. No. 105-551 (1998)	8
S. Rep. No. 105-190 (1998)	3, 6
Hearing on H.R. 2281 and H.R. 2280 Before the Subcomm. on Courts and Intellectual Property of the Comm. on the Judiciary, 105th Cong. 77 (1997) (statement of Robert W. Holleyman II, President, Business Software Alliance).	25
Pornography, Technology, and Process: Problems and Solutions on Peer-to-Peer Networks: Hearing Before the Senate Committee on the Judiciary, 108th Cong. (Sept. 9, 2003)	8

MISCELLANEOUS

Gaither, *Recording Industry Withdraws Suit*, Boston Globe, Sept. 24, 2003	17
P. Huber, *et al.*, Federal Telecommunications Law (2d ed. 1999)	4

Cited Authorities

Page

Jan 21, 2004 RIAA Press Release, *at* http://www.riaa.com/news/newsletter/012104.asp (visited June 21, 2004) 15

John Borland, *RIAA takes hundreds more 'John Does' to court*, CNET News.com (June 22, 2004), *at* http://zdnet.com.com/2102-1104_2-5243587.html? (visited June 22, 2004) 15

Inquiry Concerning the Deployment of Advanced Telecommunications Capability, 14 F.C.C.R. 2398 (1999) 8

Mar. 25, 2004 Transcript of Q&A With RIAA President Cary Sherman, *at* http://www.dailytexanonline.com/news/2004/03/25/Focus/Transcript.Of.Qa.With.Riaa.President.Cary.Sherman-641217.shtml (visited June 14, 2004) 16

http://www.alsscan.com/copyright.html 17

RIAA nearing 1,000 subpoenas against file-sharing suspects, Pioneer Press (July 18, 2003), *at* http://www.twincities.com/mld/pioneerpress/business/technology/6335275.htm?1c (visited June 21, 2004) 30

TABLE OF APPENDICES

	Page
Appendix A — Article III Of The United States Constitution	1a
Appendix B — First Amendment To The United States Constitution	3a
Appendix C — Title I Of The Digital Millennium Copyright Act Of 1998, As Codified At 17 U.S.C. §§ 1201-1205	4a
Appendix D — Title II Of The Digital Millennium Copyright Act Of 1998, As Codified At 17 U.S.C. § 512	33a

JURISDICTION

Respondent has consistently maintained that the United States District Court for the District of Columbia lacked Article III jurisdiction to issue or enforce the subpoenas at issue here because they were not issued in furtherance of the resolution of any pending case or controversy. *See, e.g., United States v. Morton Salt Co.*, 338 U.S. 632, 642-43 (1950); *United States Catholic Conf. v. Abortion Rights Mobilization, Inc.*, 487 U.S. 72, 76 (1988); *Hoffmann-La Roche, Inc. v. Sperling*, 493 U.S. 165, 172-74 (1989).

Respondent does not, however, contest the jurisdiction of the court of appeals or this Court to examine the federal questions whether these subpoenas were properly issued under the relevant statute and whether their issuance and enforcement lies outside the judicial power as defined by Article III, section 2 of the U.S. Constitution. Pet. 2a n.1, *id.* at 60a n.6; *Steel Co. v. Citizens for a Better Environment*, 523 U.S. 83 (1998). At the very least, this Court has jurisdiction to determine whether the district court had jurisdiction to conduct any subpoena enforcement proceedings, as this Court always has jurisdiction to examine its own jurisdiction and the jurisdiction of the courts below. *Marbury v. Madison*, 5 U.S. (1 Cranch) 137 (1803).

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

This matter involves the subpoena provision of the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 512(h), and implicates both Title I and Title II of the Act. Title I, *id.* §§ 1201-1205, is reprinted herein at 4a-32a; Title II, *id.* § 512, is reprinted at 33a-51a. This matter also involves Article III of the U.S. Constitution, reprinted at 1a-2a, and the First Amendment, reprinted at 3a.

SUMMARY OF REASONS FOR DENYING THE PETITION

The petition for certiorari should be denied because it satisfies *none* of the criteria specified by this Court's rules or decisions for issuance of the writ. Not surprisingly, the petition fails to cite this Court's Rule 10 or any authority that supports certiorari in the circumstances of this case. A unanimous panel of the D.C. Circuit (Ginsburg, C.J., Roberts, J., and Williams, S.J.) correctly decided a discrete issue of statutory construction by careful examination of the plain language, structure, legislative history, and purpose of the statutory provision at issue. No member of that court even called for a response to RIAA's petition for rehearing and rehearing en banc.

The court of appeals also quite properly observed that the application of copyright laws to new technologies requires a careful balancing of interests that this Court repeatedly has held is for Congress, not the federal courts, to perform. The D.C. Circuit is the first appellate court in the nation to address the scope of the DMCA's novel subpoena provision and whether it applies to new peer-to-peer technology. Its statutory analysis and conclusions are fully consistent with the decisions of this Court and do not conflict with the decision of any federal or state appellate court.

Nor are there any extraordinary circumstances that would justify deviation from this Court's normal criteria for issuance of the writ. Copyright owners possess and are vigorously employing numerous legal tools to combat on-line infringement, and Petitioner's own President has publicly stated that the D.C. Circuit's decision has not impeded RIAA's enforcement efforts in the slightest. In addition, the relevant House and Senate Committees have held extensive hearings on the proper legislative response to new peer-to-peer applications, which were not contemplated by Congress when it enacted the DMCA. For these reasons, use of this Court's limited resources to review the decision below is neither necessary nor appropriate.

STATEMENT OF THE CASE

A. Legal and Factual Background

1. The Statutory Framework and Legislative Purpose of the DMCA

The DMCA amended the Copyright Act as part of Congress's first attempt to balance copyright owners' interests in enforcing their property rights against the rights of Internet service providers and the more than 100 million individual Internet users in this country. To this end, Title I of the DMCA, entitled "Copyright Protection and Management Systems" in Title 17 of the U.S. Code, is focused primarily on helping copyright owners to protect their property rights and provides them with powerful new civil and criminal remedies to prevent the circumvention of technological "self help" measures. 17 U.S.C. §§ 1201-1204. These include protection of encryption and other access control technologies and severe penalties for falsifying, removing, or altering digital "watermarks" or other copyright management information.

Title II of the DMCA, entitled "Limitations on liability relating to material online" in Title 17, codified a set of limited immunities for Internet service providers and was intended to "ensure[] that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will expand." S. Rep. No. 105-190, at 2 (1998). These immunities, and the duties that service providers must undertake to claim them, turn entirely on the particular function the provider is performing in relation to the creation, storage, and dissemination of Internet content or material, functions that are separately described in subsections (a) through (d) of Title II. 17 U.S.C. § 512(a)-(d).

In affording distinct treatment of service providers based upon the particular functions they are performing, Title II recognizes a longstanding distinction in the law of copyright—the difference between: i) an entity acting as a passive conduit for communications created, controlled, stored, and disseminated by others; and ii) an entity storing or "hosting" material on its own system or network and itself disseminating that material to others. *Compare id.* § 512(a)

("Transitory Digital Network Communications"), *with id.* § 512(c) ("Information Residing on Systems or Network at Direction of Users"). Entities performing the former pure "transmission" or "conduit" function, such as telephone companies, have traditionally enjoyed immunity from liability for contributory infringement. *See, e.g., E. Microwave, Inc. v. Doubleday Sports*, 691 F.2d 125, 128 (2d Cir. 1982) (discussing historical "common carrier" immunity for copyright infringement); P. Huber, *et al.*, Federal Telecommunications Law 1240-55 (2d ed. 1999). Subsection (a) of Section 512, which describes the "transmission" or "conduit" function for an Internet service provider, mirrors this traditional immunity and is not conditioned on the performance of *any independent duties* by service providers.

By contrast, subsections (b), (c), and (d) of Section 512, which pertain to circumstances in which the service provider plays a relatively more active role, condition the service provider's DMCA protection on its performance of specific duties to assist copyright owners in protecting their property interests. These duties apply only in situations where the service provider has the ability to locate the particular material claimed to be infringing and to either selectively remove it or temporarily disable access to it via the Internet. In the context of subsections (b), (c), and (d), the service provider itself is storing and controlling the dissemination of some potentially infringing material on its own system or network, and—unlike the service provider who functions as a mere conduit as described in subsection (a)—has both the technical ability and the legal right to locate and alter or disable Internet access to particular material.

Subsection (c) of the statute addresses the paradigmatic situation where the service provider has substantial control over potentially infringing material. It applies to "material that resides on a system or network controlled or operated by or for the service provider," *id.* § 512(c), such as a website "hosted" on a service provider's servers. Subsection (c) establishes a "notice and take-down procedure" by which a copyright owner may notify a service provider

that material it is hosting is potentially infringing, *see id.* § 512(c)(3), and thereby require the service provider, as a condition of receiving limited immunity, to "remove, or disable access to, the material that is claimed to be infringing," *id.* § 512(c)(1)(C). The notification must specify a particular "online site" where the allegedly infringing material is located and must contain: "[i]dentification of the material that is claimed to be infringing . . . and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material." *Id.* § 512(c)(3)(A)(ii) & (iii).

The statute makes quite clear that the physical "remov[al]" of "material" or "disabling access" to "material" is a different remedy from the "termination" of a subscriber's "account." The former remedy is surgical and involves excising particular material from a website or temporarily disabling access to the material. By contrast, termination of a subscriber's account involves ending the subscriber's ability to gain any access to the Internet through that account. Subsections (j) and (i) of the statute both distinguish between these two concepts, describe them in different terms as applying to different things (*e.g.*, "material" versus "subscribers" or "accounts"), and establish very different predicates for their use. *Compare id.* § 512(j)(1)(A)(i) (authorizing injunction restraining service provider "from providing access to infringing material"), *with id.* § 512(j)(1)(A)(ii) (authorizing injunction restraining service provider "from providing access to a subscriber or account holder . . . by terminating the accounts of the subscriber or account holder"); *see also id.* § 512(i) (providing for "the termination of subscribers and account holders of the service provider's system or network who are repeat infringers").

Subsections (b) and (d) deal with storage functions where the service provider has less control over the content and correspondingly more limited duties as a precondition to statutory immunity. Subsection (b) addresses "caching," where a service provider's system automatically makes a copy of a website that is hosted elsewhere in order to facilitate ready access by its customers. Subsection (d) deals with information location tools, such as

"a directory, index, reference, pointer, or hypertext link" that refers or links users to potentially infringing material. Both subsections (b) and (d) make explicit cross-reference to the "notice and take-down procedure" established by subsection (c) and incorporate modified versions of that procedure into the service provider's duties under those subsections. *Id.* § 512(b)(2)(E), (d)(3).

Numerous provisions of Section 512, including the subpoena provision at issue in these proceedings, expressly cross-reference or incorporate concepts from the "notice and take-down" procedures established in subsection (c)(3). Thus, subsection (f) provides for damages and attorney's fees where a misrepresentation in a subsection (c)(3) notification results in the erroneous removal of or disabling of access to non-infringing material. Subsection (g) establishes a procedure for "counter notification" by the individual associated with the material that is the subject of a subsection (c)(3) notification and, unless certain conditions are met by the copyright owner, requires the service provider to restore access to the removed or disabled material. Finally, and as discussed in detail below, subsection (h), the subpoena provision at issue here, incorporates the subsection (c)(3) "notice and take-down procedure" at every stage of the subpoena process.

Subsection (a) thus stands alone among the operative provisions of the statute in that it does not provide for any notification and take-down procedure and it does not make any reference to the notice and take-down procedures contained in subsection (c)(3). In fact, subsection (a) does not impose any duties on service providers to remove or disable access to any material.

What the structure of the statute implicitly establishes both the statutory text and legislative history make explicit—the particular functions service providers are performing drive the application of all the service provider duties contained in the statute. *See id.* § 512(n) ("Subsections (a), (b), (c), and (d) describe separate and distinct functions for purposes of applying this section."); S. Rep. No. 105-190, at 19 (1998) ("In the beginning, the Committee identified the following activities: (1) digital network

communications, (2) system caching, (3) information stored on service providers, and (4) information location tools.").

Subsection (h) contains the novel subpoena provision at issue here. This provision permits a copyright owner or its representative, under very specific circumstances, to obtain a subpoena to force a service provider to turn over identifying information about a subscriber associated with specific allegedly infringing material. Consistent with the organization of Title II as a whole, subsection (h)'s application is dependent entirely on which function the service provider is performing.

Specifically, subsection (h) incorporates and relies upon the notification procedures applicable to subsections (b), (c), and (d) at each stage of the subpoena process. Subsection (h)(2), entitled "Contents of request," mandates that "a copy of the notification described in subsection (c)(3)(A)" be filed with the clerk of the court with any request for a subpoena. Subsection (h)(3), entitled "Contents of subpoena," specifies that the subpoena shall "authorize and order the service provider receiving the notification and the subpoena to expeditiously disclose . . . information sufficient to identify the alleged infringer of the material described in the notification." Subsection (h)(4), entitled "Basis for granting subpoena," provides that, "[i]f the notification filed satisfies the provisions of subsection (c)(3)(A)" and other conditions precedent, the clerk must issue and sign the proposed subpoena. Finally, subdivision (h)(5), entitled "Actions of service provider receiving subpoena," requires that "a notification described in subsection (c)(3)(A)" be served upon the service provider either with or before any DMCA subpoena.

That Congress chose to tie the subpoena provision—and the correlative duty of the service provider to disclose its subscriber's identity—to storage functions, and to the "notice and take down" procedures that are applicable only to storage functions, is not surprising. It reflects the fact that in 1998, the central problem Congress addressed was the unlawful dissemination of copyrighted material through websites hosted by service providers. The primary

remedy in the DMCA (besides copyright owner self-help that does not involve the service provider) was the take-down procedure, which is designed to "remove" particular material that is claimed to be infringing from a website or "disable access" to material pending the further procedures specified in subsection (g).

The personal communications from one Internet user to another were not viewed as a major threat to copyright holders' interests in 1998. First, peer-to-peer software, which now allows for the identification and transmission of digital files from one Internet user's computer to another's, simply did not exist in 1998. Pet. 14a-15a, 42a. Peer-to-peer software, such as "KaZaA" and "Grokster," that allows each computer to be both server and client and to search and download material from users' hard drives without utilizing a central server or directory did not arrive on the scene until after the legal demise of Napster in 2000.[1]

Second, in 1998, the vast majority of individual Internet users were limited to dial-up connections at speeds that simply did not allow for the instantaneous exchange of large digital files, such as music files in MP3 format. *See, e.g., Inquiry Concerning the Deployment of Advanced Telecommunications Capability*, 14 F.C.C.R. 2398, ¶¶ 6, 16 (1999) (broadband services at "an early stage of deployment"; only a "fledgling market" for them existed).

In addition, the limited reach of the DMCA's novel subpoena provision reflects the fact that Congress viewed those subsection (a) functions that did exist in 1998, such as email and web browsing, H.R. Rep. No. 105-551, at 42 (1998), as private

1. *See Pornography, Technology, and Process: Problems and Solutions on Peer-to-Peer Networks: Hearing Before the Senate Comm. on the Judiciary*, 108th Cong. (Sept. 9, 2003) (Statement of John Malcolm, U.S. Dep't of Justice) (distinguishing the vastly different "fisherman's net" architecture of peer-to-peer applications from the "traditional networks" in place in 1998 where "people who want[ed] to share files . . . stored them on one or more central 'servers'").

expressive activities not to be disturbed by *any* provision of the DMCA.[2] The distinction between information stored on an external network (*e.g.*, the service provider's network or system), *see* 17 U.S.C. § 512(c), and information stored on an individual's home computer, *see id.* § 512(a), reflects the higher level of subscriber privacy expectations when an Internet user stores information on a home computer or engages in other activities that do not require storage on a public server. It reflects, too, the difference between burdening service providers with the role of "copyright policeman," requiring them to invade their subscribers' privacy in the name of any private copyright enforcement efforts, and requiring service providers to exercise narrowly targeted, content-specific control over material resident on their own systems. *Id.* § 512(m)(1).

2. The Two Subpoenas at Issue in These Proceedings

RIAA caused the issuance of two subpoenas by the United States District Court for the District of Columbia under the purported authority of Section 512(h). The subpoenas were served on Verizon on July 24, 2002 and February 4, 2003. The subpoenas commanded Verizon to disclose to RIAA, under penalty of contempt, the names, addresses, and telephone numbers of two of its otherwise anonymous subscribers. RIAA claimed that Verizon's subscribers were "using Verizon's network to offer for downloading copyrighted songs through peer-to-peer software provided by KaZaA, without the copyright holders' authorization." Pet. 23a, 56a-57a.

---

2. In Title I, Congress recognized that copyright holders' use of "self-help" technologies to monitor infringement could potentially interfere with individuals' privacy on their home computers and, therefore, enacted a "Savings clause" to protect consumer privacy. 17 U.S.C. § 1205. And, in what is codified as 17 U.S.C. § 512(m) and entitled "Protection of Privacy," Title II of the DMCA makes clear that nothing in Section 512 should be construed to require a service provider to monitor its subscribers' private communications.

B. The Proceedings Below

1. The District Court's Decisions

Verizon refused to reveal its subscribers' identities to RIAA. In the first proceeding, RIAA filed a motion to enforce the subpoena, and Verizon objected on the ground that Section 512(h) does not apply to situations in which a service provider is merely performing a conduit function as described under Section 512(a).

The district court rejected Verizon's arguments, holding that the subpoena power applied to every form of expression on the Internet, including those where no potentially infringing material resides on a service provider's system or network. Pet. 26a-44a. The district court conceded that peer-to-peer file-sharing software, such as a KaZaA, was "'not even a glimmer in anyone's eye when the DMCA was enacted' by Congress in 1998." *Id.* at 42a. It nonetheless concluded that Section 512(h) should be extended to apply to situations where the service provider is performing conduit functions to avoid creating what it characterized as a "huge loophole" in the statute. *Id.* at 36a. The district court also believed that the general definition of "service provider" contained in subsection (k) of the statute was relevant to the issue of what duties are imposed by particular subsections of the statute. *Id.* at 26a-30a. Based upon these observations, the district court ordered Verizon to comply with the July 24, 2002 subpoena. *Id.* at 54a.

In the second proceeding, Verizon filed a motion to quash the February 4, 2003 subpoena on the grounds that it was issued and would be enforced outside of any "case or controversy" within the jurisdiction of the federal courts under Article III and that the bare assertion of a "good faith belief" of infringement in an *ex parte* filing with the clerk provided insufficient protection of Internet users' First Amendment rights. The district court denied Verizon's motion and ordered Verizon to comply with the February 4, 2003 subpoena. Pet. 55a-111a.

---

2. The Court of Appeals' Reversal of the District Court

With Chief Judge Ginsburg writing for a unanimous panel, the D.C. Circuit "agree[d] with Verizon's interpretation of the statute" and reversed the district court's judgments in both subpoena proceedings.[3] Pet. 2a. The court of appeals "conclude[d] from both the terms of § 512(h) and the overall structure of § 512 that . . . a subpoena may be issued only to an ISP engaged in storing on its servers material that is infringing or the subject of infringing activity." *Id.* at 6a. Because the D.C. Circuit agreed with Verizon's interpretation of the statute, it did not reach either of the constitutional arguments that were pressed and passed upon below and fully briefed on appeal. *Id.* at 2a.

First, the D.C. Circuit "agree[d] with Verizon that § 512 does not *by its terms* authorize the subpoenas issued" where Verizon was performing only the "conduit" functions addressed in Section 512(a). *Id.* at 12a (emphasis added). The court recognized that there are "three items" a copyright owner "must file . . . along with its request that the Clerk of a district court issue a subpoena," the first of which is "a 'notification of claimed infringement' identifying the copyrighted work(s) claimed to have been infringed and the infringing material or activity, and providing information reasonably sufficient for the ISP to locate the material, all as further specified in § 512(c)(3)(A)." Pet. 4a. Specifically, the notice must "identify material 'to be removed or access to which is to be disabled'" by the service provider. *Id.* at 9a (quoting 17 U.S.C. § 512(c)(3)(A)(iii)).

The court of appeals noted that "§ 512(h)(4) makes satisfaction of the notification requirement of § 512(c)(3)(A) a condition precedent to issuance of a subpoena." Pet. 9a. Because the material involved in peer-to-peer exchanges is located "in the computer (or in an off-line storage device, such as a compact disc) of an individual user," the service provider "can not remove or disable

---

3. The district court treated the two subpoena enforcement proceedings as "related matters," and its second decision applied to both cases. The court of appeals then consolidated both appeals for purposes of briefing, argument, and disposition.

one user's access to infringing material resident on another user's computer." *Id.* at 9a-10a. Nor, given the clear distinctions drawn in subsection (j), could the concept of removing or disabling access to particular material be equated with the different remedy of termination of a subscriber's account. *Id.* at 10a. Because the condition precedent to issuance of a subpoena can *never* be satisfied in the subsection (a) setting, the court of appeals reasoned that the subpoena provision itself must not apply to conduit functions. *Id.* at 11a.

Second, the court of appeals emphatically rejected both the district court's and RIAA's reliance on the definition of "service provider" in Section 512(k)(1)(B), an argument that continues to figure prominently in RIAA's petition. Pet. 19-21. The court of appeals candidly stated that this argument "borders upon the silly," *id.* at 11a, and went on to expose its fallaciousness in pointed terms:

> The details of this argument need not burden the Federal Reporter, for the specific provisions of § 512(h), which we have just rehearsed, make clear that however broadly "[internet] service provider" is defined in § 512(k)(1)(B), a subpoena may issue to an ISP only under the prescribed conditions regarding notification. Define all the world as an ISP if you like, the validity of a § 512(h) subpoena still depends upon the copyright holder having given the ISP, however defined, a notification effective under § 512(c)(3)(A).

Id. at 11a-12a.

Third, the D.C. Circuit analyzed the *structure* of Section 512 as a whole, and in particular the difference between the storage functions addressed in subsections (b) through (d) and the distinct transmission function covered by subsection (a). The court explained that Section 512(h)'s three cross-references to Section 512(c)'s notice requirement could be given meaning and effect in the context of subsections (b), (c), and (d), but *could not be given any meaning or effect in the context of subsection (a)*. *Id.* at 12a-14a. The court thus concluded that "the references to § 512(c)(3)"

in subsections (b) through (d) "lead inexorably to the conclusion that § 512(h) is structurally linked to the storage functions of an ISP and not to its transmission functions, such as those listed in § 512(a)." *Id.* at 14a.

Fourth, the D.C. Circuit found that it

> need not . . . resort to investigating what the 105th Congress may have known because the text of § 512(h) and the overall structure of § 512 *clearly establish* . . . that § 512(h) does not authorize the issuance of a subpoena to an ISP acting as a mere conduit for the transmission of information sent by others.

Id. at 14a (emphasis added). Nonetheless, the D.C. Circuit did examine RIAA's proffered "legislative history" and concluded that, "the legislative history of the DMCA betrays no awareness whatsoever that internet users might be able directly to exchange files containing copyrighted works." *Id.* Quite simply, the court concluded: "Congress had no reason to foresee the application of § 512(h) to [peer-to-peer] file sharing, nor did they draft the DMCA broadly enough to reach the new technology when it came along." *Id.* at 15a.

Finally, the D.C. Circuit rejected RIAA's invitation to "rewrite the DMCA in order to make it fit a new and unforeseen internet architecture, no matter how damaging that development has been to the music industry." *Id.* at 16a. The court invoked this Court's teaching in *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417 (1984), and held that "[t]he plight of copyright holders must be addressed in the first instance by the Congress" because "only the 'Congress has the constitutional authority and the institutional ability to accommodate fully the varied permutations of competing interests that are inevitably implicated by such new technology.'" Pet. 16a (quoting *Sony*, 464 U.S. at 431).

REASONS FOR DENYING THE PETITION

I. The Petition Meets None Of The Established Justifications For Intervention By This Court.

A. There Is No Split of Authority on the Narrow Statutory Issue Resolved by the D.C. Circuit.

More than four years after the DMCA was enacted, RIAA brought these proceedings, admittedly as "test case[s]," Pet. 19a, to advance a novel and expansive interpretation of the scope of Section 512(h). RIAA concedes that the D.C. Circuit is the first court of appeals in the nation to address the scope of the DMCA's unique subpoena provision. Pet. 14. Thus, RIAA can lay claim to no conflict with the decisions of this Court or *any* appellate court, state or federal. In fact, not only is the D.C. Circuit the first appellate court to construe this particular statutory provision, but RIAA itself candidly acknowledges that the "identical issues" are now being considered in other circuits. *Id.*

Just this month, the Eighth Circuit heard oral argument in *RIAA v. Charter Communications, Inc.*, No. 03-3802 (8th Cir.), to determine whether the district court in that case erred in enforcing a DMCA subpoena where the service provider was performing only the "conduit functions" specified in Section 512(a). The same legal issues are also now before a district court in the Fourth Circuit, where the parties completed briefing last month and are awaiting the district court's decision in the context of motions to quash filed by the Internet subscribers themselves. *In re Subpoena to Univ. of N.C.*, No. 1:03mc138 & *In re Subpoena to N.C. State Univ.*, No. 1:03mc139 (M.D.N.C.).

In short, there is not now and there may never be any conflict in the circuits or confusion over the meaning of this statutory provision. At a minimum, this Court should allow continuation of the normal process whereby multiple circuits are encouraged to address a novel legal issue before any intervention by this Court. Whether even an intercircuit conflict would warrant review—where Congress is best suited to conduct, and actively interested in conducting, the careful

fact-intensive policy examination of new circumstances needed for forward-looking resolution—can be left for another day.

B. No Extraordinary Circumstances Justify Review.

This case presents no issue of immediate public importance that would itself justify review. RIAA's implication that the urgency of the "social problem," Pet. 17, of peer-to-peer file sharing demands review is belied by RIAA's own actions in the wake of the D.C. Circuit's decision. Far from being left without the ability to "fight back," RIAA has available to it, and *has extensively and successfully utilized*, the so-called "John Doe" procedure for identifying alleged infringers.

The filing of a John Doe suit, along with a motion for third-party discovery of the identity of the defendant "John Doe" is the traditional means to invoke the power of the federal courts against an otherwise anonymous defendant. Armed with this alternative legal tool, a month after the D.C. Circuit issued its decision, RIAA President Cary Sherman was able confidently to announce that RIAA's "campaign against illegal file sharers *is not missing a beat*. . . . [W]e can and will continue to bring lawsuits on a regular basis against those who illegally distribute copyrighted music." Jan 21, 2004 RIAA Press Release, *at* http://www.riaa.com/news/newsletter/012104.asp (visited June 21, 2004) (emphasis added).

Since the D.C. Circuit opinion issued, the recording industry has filed "John Doe" lawsuits against more than 3,000 alleged infringers, in well over a dozen district courts across the country. As a direct result of those efforts, RIAA has settled disputes with approximately 600 individuals, *see* John Borland, *RIAA takes hundreds more 'John Does' to court*, CNET News.com (June 22, 2004), *at* http://zdnet.com.com/2102-1104_2-5243587.html? (visited June 22, 2004), and its members have proceeded with lawsuits against named individuals who did not settle, some of which already have resulted in awards of infringement damages and permanent injunctions. *See, e.g., Arista Records, Inc. v. Brothers*, No. 3:03cv2081(JCH) (D. Conn. Apr. 30, 2004).

Moreover, since the advent of these John Doe cases, Mr. Sherman has publicly stated that RIAA has "seen a marked decline in illegal file-sharing, a marked increase in business at the legitimate online music services, and a spike in CD sales as well." Mar. 25, 2004 Transcript of Q&A With RIAA President Cary Sherman, *at* http://www.dailytexanonline.com/news/2004/03/25/Focus/Transcript.Of.Qa.With.Riaa.President.Cary.Sherman-641217.shtml (visited June 14, 2004). RIAA's preference for one legal tool over another in protecting the business interests of its members is not the kind of national legal crisis that warrants a grant of certiorari.

C. RIAA's Policy Arguments Regarding New Technologies and Requests To Expand Copyright Protections Are Properly Addressed to Congress, Not to this Court.

The D.C. Circuit did not, as RIAA suggests, strike down a federal statute or "gut[]" or "blow[] a hole in" the DMCA's subpoena provision. Pet. 15, 19, 27. The court engaged in a routine exercise in statutory construction, focusing on the plain language of the subpoena provision, its place in the statutory scheme as a whole, and the state of Internet technology and evidence regarding the scope of the problem Congress believed it was addressing in 1998. None of these traditional tools of statutory construction even hinted that the subpoena provision was written or intended to address the new problem of peer-to-peer file sharing as it exists today. Nothing in the court of appeals' opinion prevents copyright owners or their agents from using both the "take down" and subpoena provisions for all the functions addressed in subsections (b), (c), and (d).

At bottom, RIAA is asking this Court to alter the words of the subpoena provision, the structure of Section 512 as a whole, and the balance among the rights of copyright holders, Internet service providers, and Internet users that Congress struck based upon the evidence before it in 1998. The court of appeals and the district court both agreed on one historical fact that no amount of RIAA revisionist history can change: "[T]he legislative history of the DMCA

betrays no awareness whatsoever that internet users might be able to directly exchange files containing copyrighted works. That is not surprising; P2P software was 'not even a glimmer in anyone's eye when the DMCA was enacted.'" Pet. 14a (quoting Pet. 42a).

As the D.C. Circuit properly recognized, the job of expanding copyright protections in light of new technologies is uniquely the province of Congress, which has the institutional competence to engage in meaningful fact-finding and to balance the competing interests implicated by peer-to-peer file-sharing. Pet. 16a. Indeed, faced with the record that has unfolded since Congress first enacted the DMCA—including, *inter alia*, the susceptibility of the DMCA subpoena process to mistakes (through human error or the use of pre-programmed robotic tools to search for alleged infringement), and abuse of the process by alleged copyright owners that are significantly less responsible than RIAA[4]—it is far from a forgone conclusion that Congress would place the interests of copyright owners in a streamlined subpoena tool over the interests of Internet

---

4. The record below is filled with evidence of mistakes by copyright owners and their representatives and examples of potential abuses of the cursory DMCA subpoena process. One copyright bounty hunter mistook a file entitled "Harry_Potter_Book_Report.rtf" for an infringing copy of the movie *Harry Potter and the Sorcerer's Stone.* The file was in fact a child's book report, but the robotic program the bounty hunter used to search the Internet for potential copyright infringement could not tell the difference. In the proceedings below, RIAA even submitted a sworn declaration of a pornography purveyor, ALS Scan, who averred to its use of the DMCA subpoena process in protecting its copyrighted works. *See* http://www.alsscan.com/copyright.html (claiming copyright in hundreds of pornographic images). After the case was submitted to the D.C. Circuit, RIAA obtained and executed a DMCA subpoena based upon its "good faith belief" that a subscriber had downloaded over 2,000 songs, and then filed an infringement action against the identified subscriber seeking damages of up to $150,000 per song. As it turned out, the defendant, whose privacy and anonymity were improperly breached, was a 66-year-old grandmother who does not even own a computer capable of running file-sharing software. *See* Gaither, *Recording Industry Withdraws Suit*, Boston Globe, Sept. 24, 2003, C1.

users in protecting their privacy in communications stored on their home computers.

Copyright owners repeatedly have sought to have the federal courts "adapt" existing law to cover new technologies that *they perceive* as a threat to their business interests. This Court has repeatedly declined such invitations, finding that the adjustment of rights necessary where new technologies alter the market for copyrighted works is, as a matter of both textual commitment and institutional competence, for Congress alone to decide:

> Sound policy, as well as history, supports our consistent deference to Congress when major technological innovations alter the market for copyrighted materials. Congress has the constitutional authority and the institutional ability to accommodate fully the varied permutations of competing interests that are inevitably implicated by such new technology.

Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 431 (1984).

Just last Term, this Court reiterated its commitment to "defer substantially to Congress" on copyright issues and reaffirmed that "it is generally for Congress, not the courts, to decide how best to pursue the Copyright Clause's objectives." *Eldred v. Ashcroft*, 537 U.S. 186, 204 (2003) (citing *Sony*, 464 U.S. at 429, and *Stewart v. Abend*, 495 U.S. 207, 230 (1990)). Consistent with this well-established principle of judicial restraint in the copyright field, this Court should decline RIAA's invitation to use a statute that is almost six years old to wade into an ongoing legislative debate about how to address the latest developments in Internet technology. The issue should be left with Congress, which, as the D.C. Circuit noted, Pet. 16a, is presently conducting hearings regarding peer-to-peer technologies and considering possible legislative responses to them.

II. The Court Of Appeals Correctly Applied Settled Canons Of Statutory Construction.

A. The Text, Structure, History, and Purpose of Section 512 Compel the Result Reached by the D.C. Circuit.

A unanimous panel of the D.C. Circuit correctly resolved what RIAA itself describes as "a straightforward issue of statutory construction." Pet. 17. Try as it might, RIAA is unable to offer this Court a coherent and logical interpretation of subsection (h) in particular, or of Section 512 in general, that is consistent with its litigation position. The statute can only get RIAA where it wants to go through a less than subtle form of result-oriented bending and twisting that runs counter to basic canons of statutory construction. In the end, RIAA's arguments fail even to address, let alone cast doubt upon, the court of appeals' careful statutory analysis.

1. The Text and Structure of Section 512 Compel the Conclusion That Section 512(h) Applies Only to Material Stored on a Service Provider's System or Network.

Under the plain language of Section 512(h), the issuance of a subpoena to compel a service provider to disclose confidential information about its subscriber's identity is conditioned on the filing and service of a valid take-down notification described in subsection (c)(3)(A). Thus, the scope and application of subsection (h) is dependent on: i) whether the notification and take-down procedure applies to the particular function at issue; and ii) whether both the copyright owner and the service provider can comply with the requirements of, and obligations created by, the notice and take down procedure as specified in subsection (c)(3)(A).

On its face, subsection (h) contains three separate cross-references to the subsection (c)(3)(A) take-down notice, 17 U.S.C. § 512(h)(2)(A), (h)(4), (h)(5), and expressly makes "satisf[action of] the provisions of subsection (c)(3)(A)" a condition precedent to the issuance of every Section 512(h) subpoena, *id.* § 512(h)(4). In turn, the required subsection (c)(3)(A) notice, the statute says, can "be effective" only if it allows the service provider to "locate"

and "remove" or "disable[]" "access to" "the material that is claimed to be infringing." *Id.* § 512(c)(3)(A)(iii).

As the D.C. Circuit concluded, these statutory requirements for the issuance of a Section 512(h) subpoena cannot have any force or effect in the subsection (a) context. The statute does not authorize any subsection (a) take-down notices, and a service provider performing conduit functions under subsection (a) has neither the technical ability nor the legal right to locate and selectively remove or disable Internet access to material residing on the personal computers of individual subscribers. Pet. 9a-10a.

In order to accept RIAA's reading of the statute (*i.e.*, that subsection (h) applies regardless of the service provider's function), one must ignore the fact that Congress omitted any notice and take-down provisions from subsection (a). RIAA's construction renders Section 512(h)'s numerous cross-references to *material* that is the subject of a subsection (c)(3)(A) notice (material which the service provider must be able to locate, remove, or disable access to) so much congressional gibberish because that kind of material can never exist in the subsection (a) context. Under RIAA's reading of the statute, Congress required the filing and service of a meaningless document that could never "satisf[y] the provisions of subsection (c)(3)(A)," *id.* § 512(h)(4), and could never obligate the service provider to do anything. In addition, the damages remedy for a misrepresentation that particular material is infringing in subsection (f) applies only where the service provider is able to remove or disable access to the material and thus would *never* apply to representations made to obtain a subpoena in the subsection (a) context. The limits on this important protection for subscribers further confirms that Congress was addressing only storage functions in subsection (h). The only coherent reading of Section 512(h) is that its cross-references to subsection (c)'s take-down notice *do* have meaning and effect, because

Section 512(h) applies only to storage functions where a take-down notice is provided for and can be effective.[5]

While the D.C. Circuit carefully adhered to this Court's instructions regarding holistic construction of statutes to arrive at a logical and harmonious whole, *see, e.g., FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 133 (2000), the petition quite consciously eschews this approach and instead attempts to poke holes in the D.C. Circuit's opinion by reading isolated statutory provisions out of context. Each one of these attempts is futile.

First, RIAA argues that the D.C. Circuit erred when it determined that a service provider performing conduit functions under subsection (a) is unable to "remove" or "disable access to" the allegedly offending material. Pet. 22-23. In support of this theory, RIAA posits that the service provider in the subsection (a) context could, *in lieu of* removing or disabling access to the content at issue, terminate the subscriber's account entirely, thereby preventing the subscriber from sending or receiving *any content at all* over the Internet. *Id.*

Not only does this suggestion impute to Congress an implausible intent to require the radical step of termination of all Internet access based only upon an *ex parte* assertion of a "good faith belief" that some material may be infringing, it also ignores the care with which Congress distinguished between requiring a service provider surgically to remove or disable access to particular material and the altogether different remedy of requiring a service provider to terminate a subscriber's account. *See* 17 U.S.C. § 512(j)(1)(B)(i) (referring to injunctive relief that requires "terminating the accounts of the subscriber"). To ignore this distinction is to violate the elementary canon of statutory interpretation that different words in

---

5. A statutory cross-reference is a well-recognized mechanism for incorporating procedures or limitations from another part of the same statute. *E.g., Overseas Educ. Ass'n v. FLRA*, 824 F.2d 61, 65 (D.C. Cir. 1987); *Estate of Joseph Leder v. Comm'r of Internal Revenue*, 893 F.2d 237, 241 (10th Cir. 1989).

the same statute are to be interpreted differently. *Williams v. Taylor*, 529 U.S. 362, 404 (2000).

It is no answer that statutory terms can have "overlapping" meanings. Pet. 22-23 & n.16. The general proposition that some overlap of statutory terms is theoretically possible says nothing about the correct interpretation and interrelationship of the specific terms used in Section 512. Even if overlap exists, it does nothing to undermine the distinct nature of the terms as employed in the relevant provisions of this statute.[6] Thus, compared with removing or disabling access to material, which the service provider can do in a precise manner when it hosts that material, and which the service provider may have a further obligation to undo under subsection (g), termination of a subscriber's account is often a broader remedy—ending the subscriber's ability to send or receive any material over the Internet. Pet. 10a. It could also be viewed as a narrower remedy in the sense that it may not remove access to particular material at all if the subscriber has another means of Internet access to receive or disseminate that material. Many terms in the English language have some conceptual overlap, but that general proposition cannot undermine a specific choice by Congress in a particular statute to invoke one term or concept in some places and another term or concept in others.

In Section 512, the termination of accounts is referenced in several places, *see* 17 U.S.C. § 512(j)(1)(A)(ii), (j)(1)(B)(i), (i)(1)(A), but never in the context of a take-down notice or the

---

6. Indeed, even within subsection (j) itself, Congress distinguished between "[a]n order restraining the service provider from providing access to *infringing material or activity* residing at a particular online site on the provider's system or network," 17 U.S.C. § 512(j)(1)(A)(i) (emphasis added), and one "restraining the service provider from providing access to a subscriber . . . of the service provider's *system or network* who is engaging in infringing activity . . . , by terminating the accounts of the subscriber," *id.* § 512(j)(1)(A)(ii) (emphases added). Moreover, Congress reserved the extreme remedy of account termination for repeat infringers or those subject to a court order. *Id.* § 512(i), (j). No such remedy is provided for "alleged infringers," *id.* § 512(h)(1), who can be the subject of Section 512(h) subpoenas.

subpoena provision. By contrast, the terms "remove" and "disable access" are used exclusively in provisions that address storage functions, where the service provider has access to and control of the material at issue. *See, e.g.*, § 512(b)(2)(E), (c)(1)(C), (c)(3)(A)(iii), (d)(3), (f)(2), (g)(1)&(2). The removal of or disabling of access to particular material cannot be equated with the termination of a subscriber's account without doing violence to both the text and structure of the statute.

Second, RIAA argues that the D.C. Circuit's reading of the subpoena provision "is contradicted by" subsection (h)(5). Pet. 21-22. Subsection (h)(5) not only fails to support RIAA's position but provides *further proof* that the subpoena provision does not apply to the subsection (a) context. Subsection (h)(5) includes one of the three express cross-references to the notification in subsection (c)(3)(A) and states that, "[u]pon receipt of the issued subpoena . . . , the service provider shall" disclose the information sought, "regardless of whether the service provider responds to the notification." 17 U.S.C. § 512(h)(5).

To the extent this last clause of subsection (h)(5) bears on the content or effect of the notification at all, it undermines RIAA's position because the negative implication of the clause is that subpoenas will be issued only in circumstances where a service provider *could* effectively respond to the notification, even if it chooses not to do so. Subsection (h)(5) also contemplates that a take-down notification might be served *before* a subpoena, which of course makes no sense if the take-down notice is purely "informational" and its only purpose is to obtain the subpoena. Pet. 21-22.

Finally, RIAA posits that the D.C. Circuit erred by not giving adequate weight to the definition of "service provider" in the statute. Pet. 20-21. The use of the generic definition of "service provider" in 512(h) simply means no service provider is excluded from Section 512(h) at the threshold definitional level. It is a non sequitur to say that, for that reason, a subpoena can be issued under Section 512(h) when the provision's express *requirements* are not met.

Those requirements, as described, include the hosting requirement. RIAA's argument, the D.C. Circuit correctly concluded, "borders upon the silly." Pet. 11a.

2. The Legislative History and Purpose of the Statute Further Confirm That Section 512(h) Does Not Apply to the Conduit Context.

This is a case where "the plain language" of the DMCA should "mark[] the beginning and end" of the judicial inquiry. *U.S. R.R. Ret. Bd. v. Fritz*, 449 U.S. 166, 176 (1980). Unable to reconcile its preferred interpretation with the text and structure of Section 512, RIAA devotes the bulk of its petition to arguing that Congress could not possibly have intended to limit the subpoena provision to storage functions and that adhering to the plain language and structure of the statute frustrates congressional purpose (as now defined by RIAA more than four years after the statute was enacted). Pet. 15-19, 23-24.

RIAA cannot deny that the peer-to-peer architecture was not contemplated by Congress in 1998 and instead relies on scattered snippets of congressional testimony, generally drawn from spokespersons for copyright owners or from discussions of legislation *other than the DMCA*[7] to suggest that Congress had some premonition about copyright problems that could arise in the conduit context. Not only are the self-serving statements of copyright owners a poor guide to statutory interpretation, *see, e.g., S&E Contractors, Inc. v. United States*, 406 U.S. 1, 13 n.9 (1972), but even those statements RIAA has chosen to

---

7. *See, e.g.*, Pet. 3-4 (citing to hearings regarding an amendment to the criminal provisions of the Copyright Act that had nothing to do with service provider duties under Title II of the DMCA); *id.* at 6 (same); *id.* at 6 n.8 (statement of songwriter); *id.* at 8 n.11 (quoting testimony of RIAA's General Counsel). RIAA also cites pre-enactment news articles that it claims discuss technologies antecedent to peer-to-peer file sharing. *E.g.*, Pet. 4-5. These news reports may reflect what technology experts were anticipating in the development of Internet technologies, but they offer no support for the proposition that Congress considered, let alone attempted to address, these issues in 1998.

highlight do not connect the subsection (a) functions to the subpoena provision.[8]

Finally, RIAA argues that the views of the Register of Copyrights, expressed in a legislative hearing five years after the DMCA was enacted, are "entitled to deference." Pet. 16 & n.14. This is interpretive desperation. The Register has been delegated no authority to interpret or apply Section 512(h), and her testimony relies on RIAA's and the district court's flawed interpretation of Section 512(h). Thus, the Register's testimony on this issue of statutory construction is not entitled to any weight in this Court. *See, e.g., United States v. Mead Corp.*, 533 U.S. 218, 227, 231 (2001); *Christensen v. Harris County*, 529 U.S. 576, 587 (2000).

B. The D.C. Circuit's Reading of the Statute Avoids Serious First Amendment Concerns.

Because the D.C. Circuit agreed with Verizon's position that the subpoena provision does not apply to the conduit context, the court properly declined to reach the First Amendment issues decided by the district court. Pet. 2a. To the extent there is any doubt as to whether the subpoena provision should be read to apply to the conduit context, the D.C. Circuit properly avoided the serious First Amendment concerns presented by an expansive reading of this unique subpoena power.

As the district court correctly concluded, Pet. 79a-82a, there can be no doubt that Internet users have a First Amendment right to speak and associate anonymously. *See, e.g., McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 341-42 (1995). By design, at the time Section 512(h) is invoked, there has been no judicial determination of copyright infringement and thus the Internet speaker

---

8. Indeed, the only testimony of the type RIAA draws upon that connects the sharing of information about "the infringer's identity" to a particular function ties it to "material [located at] a particular site on a service provider's system." *Hearing on H.R. 2281 and H.R. 2280 Before the Subcomm. on Courts and Intellectual Property of the Comm. on the Judiciary*, 105th Cong. 77 (1997) (statement of Robert W. Holleyman II, President, Business Software Alliance).

who is the subject of the subpoena must be presumed to be engaged in fully protected speech and association. Because Section 512(h) is a procedure designed to strip Internet users of this presumptively protected anonymity, "those procedures violate the First Amendment unless they include built-in safeguards against curtailment of constitutionally protected expression, for Government 'is not free to adopt whatever procedures it pleases for dealing with [illicit content] without regard to the possible consequences for constitutionally protected speech.'" *Blount v. Rizzi*, 400 U.S. 410, 416 (1971).[9]

Section 512(h) on its face includes no such protections and, under RIAA's reading, would permit the employment of a federal court's power to strip Internet users of their anonymity upon no more than an *ex parte*, subjective "good faith" statement by anyone willing to claim that he or she is a copyright owner or the owner's representative and that some form of copyright infringement *might* be occurring. 17 U.S.C. § 512(c)(3)(A)(v). Such a cursory showing is not sufficient to shift the burden to the service provider (who does not even have access to the material) to defend the First Amendment rights of its subscriber. *See, e.g., Blount*, 400 U.S. at 418. Under any level of First Amendment scrutiny, this process fails the requirement that laws restricting speech be narrowly tailored to impose the least burden on protected speech and that the advocate of suppression of speech or association bear the burden of proof. *Freedman v. Maryland*, 380 U.S. 51, 58-60 (1965); *Philadelphia Newspapers, Inc. v. Hepps*, 475 U.S. 767, 775-78 (1986).

Finally, even if these serious First Amendment concerns did not raise doubts about the subpoena provision as a whole, they further support the D.C. Circuit's conclusion that subsection (h) does not apply to the conduit context. Under the D.C. Circuit's reading, those activities where the subscriber's privacy and anonymity interests

---

9. It is for this reason that federal courts have demanded that those who would seek to strip Internet users of their anonymity must not merely file a complaint, but also must demonstrate that their allegations can withstand heightened judicial scrutiny. *E.g., Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 579-80 (N.D. Cal. 1999).

are at their zenith, in connection with material stored on the subscriber's own home computer, are not subject to Section 512(h)'s truncated process. *See, e.g., Stanley v. Georgia*, 394 U.S. 557, 564 (1969) (expressive activity that may be proscribed outside the home is constitutionally protected inside the home). In addition, where the material resides on the service provider's system or network, the service provider can examine the material and come to a judgment about the infringement claim. Finally, only in the context of an effective take-down notice are the protections of subsections (f) and (g) available to the subscriber. The fact that the D.C. Circuit's reading of the statute comports with *both* traditional canons of statutory construction *and* principles of constitutional avoidance confirms that this Court's review is neither necessary nor likely to lead to a different outcome.

C. The Existence of a Substantial Alternative Ground for Affirming the Judgment Below Militates Against Granting the Petition.

Because it agreed with Verizon's reading of the statute, the court of appeals did not address another issue that was decided by the district court and fully briefed on appeal—the question whether the issuance of these subpoenas outside of any pending case or controversy within the meaning of Article III of the U.S. Constitution renders them void and unenforceable.[10] The D.C. Circuit's judgment vacating the district court's orders could be affirmed on the alternative ground that, regardless of the scope of Section 512(h), Congress cannot authorize an Article III court to issue or enforce binding legal process outside of a pending case or controversy. This independent ground for affirmance further counsels in favor of denying certiorari in this case.[11]

---

10. The D.C. Circuit took no position on whether the district court had jurisdiction under Article III to *issue* the subpoenas and instead exercised its jurisdiction over the district court's orders enforcing those subpoenas. Pet. 2a n.1; *see Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83 (1998).

11. Because Verizon does not seek to alter the D.C. Circuit's judgment, Verizon respectfully submits that its Article III arguments (Cont'd)

As interpreted and applied by the district court, Section 512(h) allows for the issuance of a subpoena *duces tecum* on an *ex parte* basis in the absence of a pending case or controversy. The subpoena is then subject to enforcement by an Article III court—without any lawsuit ever being filed (or even promised) and without any attempt to invoke the subject matter jurisdiction of the federal courts to resolve any issue of federal law. Judicial officers are thus engaged in purely investigative duties that are constitutionally reserved to grand juries or administrative agencies. From the Framers' time to the present, this Court consistently has held that Article III forbids the use of the federal courts as free floating investigative bodies to discover facts unconnected to the adjudication of actual cases or controversies.[12]

In *Morton Salt*, this Court made clear that "[t]he *judicial* subpoena power not only is subject to specific constitutional limitations . . . but also is subject to those *limitations inherent in the body that issues them* because of the provisions of the Judiciary Article of the Constitution." 338 U.S. at 642 (emphases added). The Court reaffirmed this principle in *Catholic Conference*, holding that "if a district court does not have subject-matter jurisdiction over the underlying action, and the *process was not issued* in aid of

---

(Cont'd)
are properly before the Court as an alternative ground for affirmance. *Bennett v. Spear*, 520 U.S. 154, 166-67 (1997). Out of an abundance of caution, Verizon has also filed a conditional cross-petition squarely placing the Article III issue before the Court.

12. *E.g.*, *Hayburn's Case*, 2 U.S. (2 Dall.) 408 (1792); *Marbury v. Madison*, 5 U.S. (1 Cranch) 137, 171-72 (1803); *United States v. Ferreira*, 54 U.S. (13 How.) 40 (1851); *Yale Todd's Case*, *printed at* 54 U.S. (13 How.) 52 (1851); *Gordon v. United States*, 117 U.S. Appx. 697, 699-706 (1864); *Muskrat v. United States*, 219 U.S. 346, 353-63 (1911); *United States v. Morton Salt*, 338 U.S. 632, 641-42 (1950); *United States Catholic Conf. v. Abortion Rights Mobilization, Inc.*, 487 U.S. 72, 76 (1988); *Hoffmann-La Roche Inc. v. Sperling*, 493 U.S. 165, 174 (1989).

determining that jurisdiction, then the process is void and an order of civil contempt based on refusal to honor it must be reversed." 487 U.S. at 76 (emphasis added).

The district court recognized that "'[f]ederal judicial power itself extends only to adjudication of cases and controversies and it is natural that its investigative powers should be jealously confined to these ends.'" Pet. 60a. It further recognized that, "at the time of issuance, a § 512(h) subpoena will not necessarily be tethered to a present or even anticipated 'adversary proceeding, involving a real, not a hypothetical, controversy' over providing the name." Pet. 74a n.12. Thus, the district court *conceded that no Article III case or controversy was present when the underlying DMCA subpoenas were issued*, but it nonetheless refused to apply the teachings of *Morton Salt* and *Catholic Conference*.

In order to reach the conclusion that Section 512(h) was constitutional, the lower court endorsed the extraordinary proposition that "the clerk's issuance of a § 512(h) subpoena does not involve either the exercise of judicial power or the exercise by federal judges of Article I or Article II-type investigatory power." Pet. 61a. Based upon its belief that the issuance of a Section 512(h) subpoena is "a quintessentially ministerial duty," *id.*, the district court apparently concluded that it does not involve the exercise of the constitutional power of *any* branch of government.

This transparent attempt to side-step well-established limitations on the judicial power must be rejected. The two subpoenas here were issued *in the name of the district court* and carried with them *on the day of their issuance* the enforcement authority that federal courts derive only from Article III of the Constitution. Under the district court's reasoning, as long as the clerk initiates the process, Article III courts can be pulled into myriad purely investigative duties that are clearly forbidden to them by the Constitution.

Finally, beyond the *per se* violation of the requirements of Article III, legislative cooptation of federal judicial clerks for non-judicial duties raises a host of *additional* separation of powers concerns. The clerks of any federal court, including this one, are inferior officers

of the Judicial Branch. 28 U.S.C. § 956; *see Buckley v. Valeo*, 424 U.S. 1, 126 (1976). The assignment of extra-judicial duties to an inferior judicial officer is, in itself, an intrusion into the powers and organization of the Judicial Branch and would necessarily lead to bizarre consequences. The court could be forced to review the clerk's actions for an abuse of discretion or clear error when those actions are authorized by Article I as opposed to Article III. Moreover, the clerk's office would have to decide whether to give priority to the investigative work assigned to it by Congress over the adjudicative work assigned to it by Article III judges.

The district court itself recognized the concern that subpoenas would divert the resources of inferior judicial officers from the work of the courts, but found that at the time of its ruling "no such barrage of requests has occurred." Pet. 73a. Yet in the time between the district court penning those words and the D.C. Circuit's decision reversing the district court on the merits, the district courts were flooded with approximately 4,000 DMCA subpoena requests, such that a spokesperson for the Administrative Office of the U.S. Courts described one clerk's office as "functioning more like a clearing house, issuing subpoenas for all over the country." *RIAA nearing 1,000 subpoenas against file-sharing suspects*, Pioneer Press (July 18, 2003), at http://www.twincities.com/mld/pioneerpress/business/technology/6335275.htm?1c (visited June 21, 2004). In fact, the DMCA subpoenas were "so prolific that the" district court, "already suffering staff shortages, [was] forced to reassign employees from elsewhere in the clerk's office to help process paperwork." *Id.* For these reasons, the district court clearly erred in its Article III analysis, which provides an alternative ground for this Court to affirm the judgment below and a further reason to deny RIAA's petition.

CONCLUSION

For the foregoing reasons, Verizon respectfully submits that the petition for writ of certiorari should be denied. If this Court grants the petition, it should adopt the counter-questions presented and grant Verizon's conditional cross-petition filed concurrently herewith.

Respectfully submitted.

JOHN THORNE*
SARAH B. DEUTSCH
THOMAS M. DAILEY
LEONARD CHARLES SUCHYTA
VERIZON COMMUNICATIONS INC.
1515 N. Courthouse Road
Fifth Floor
Arlington, Va. 22201
(703) 351-3900

ANDREW G. MCBRIDE
KATHRYN COMERFORD TODD
BRUCE G. JOSEPH
KARYN K. ABLIN
DINEEN PASHOUKOS WASYLIK
WILEY REIN & FIELDING LLP
1776 K Street NW
Washington, D.C. 20006
(202) 719-7000

Attorneys for Respondent

* *Counsel of Record*

June 25, 2004

APPENDIX

APPENDIX A

ARTICLE III OF THE UNITED STATES CONSTITUTION

Section 1.

The judicial Power of the United States, shall be vested in one supreme Court, and in such inferior Courts as the Congress may from time to time ordain and establish. The Judges, both of the supreme and inferior Courts, shall hold their Offices during good Behaviour, and shall, at stated Times, receive for their Services, a Compensation, which shall not be diminished during their Continuance in Office.

Section 2.

The judicial Power shall extend to all Cases, in Law and Equity, arising under this Constitution, the Laws of the United States, and Treaties made, or which shall be made, under their Authority;—to all Cases affecting Ambassadors, other public ministers and Consuls;—to all Cases of admiralty and maritime Jurisdiction;—to Controversies to which the United States shall be a Party;—to Controversies between two or more States;—between a State and Citizens of another State;—between Citizens of different States;—between Citizens of the same State claiming Lands under Grants of different States, and between a State, or the Citizens thereof, and foreign States, Citizens or Subjects.

In all Cases affecting Ambassadors, other public Ministers and Consuls, and those in which a State shall be Party, the supreme Court shall have original Jurisdiction. In all the other Cases before mentioned, the supreme Court shall have appellate Jurisdiction, both as to Law and Fact, with such Exceptions, and under such Regulations as the Congress shall make.

Appendix A

The Trial of all Crimes, except in Cases of Impeachment, shall be by Jury; and such Trial shall be held in the State where the said Crimes shall have been committed; but when not committed within any State, the Trial shall be at such Place or Places as the Congress may by Law have directed.

Section 3.

Treason against the United States, shall consist only in levying War against them, or in adhering to their Enemies, giving them Aid and Comfort. No Person shall be convicted of Treason unless on the Testimony of two Witnesses to the same overt Act, or on Confession in open Court.

The Congress shall have Power to declare the Punishment of Treason, but no Attainder of Treason shall work Corruption of Blood, or Forfeiture except during the Life of the Person attainted.

APPENDIX B

FIRST AMENDMENT TO THE UNITED STATES CONSTITUTION

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

APPENDIX C

TITLE I OF THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998, AS CODIFIED AT 17 U.S.C. §§ 1201-1205

Chapter 12: Copyright Protection and Management Systems

Section 1201. Circumvention of copyright protection systems

(a) Violations regarding circumvention of technological measures.

- (1)(A) No person shall circumvent a technological measure that effectively controls access to a work protected under this title. The prohibition contained in the preceding sentence shall take effect at the end of the 2-year period beginning on the date of the enactment of this chapter.

(B) The prohibition contained in subparagraph (A) shall not apply to persons who are users of a copyrighted work which is in a particular class of works, if such persons are, or are likely to be in the succeeding 3-year period, adversely affected by virtue of such prohibition in their ability to make noninfringing uses of that particular class of works under this title, as determined under subparagraph (C).

(C) During the 2-year period described in subparagraph (A), and during each succeeding 3-year period, the Librarian of Congress, upon the recommendation of the Register of Copyrights, who shall consult with the Assistant Secretary for Communications and Information of the Department of Commerce and report and comment on his or her views in making such recommendation, shall make the determination in a rulemaking proceeding for purposes of subparagraph (B)

of whether persons who are users of a copyrighted work are, or are likely to be in the succeeding 3-year period, adversely affected by the prohibition under subparagraph (A) in their ability to make noninfringing uses under this title of a particular class of copyrighted works. In conducting such rulemaking, the Librarian shall examine –

(i) the availability for use of copyrighted works;

(ii) the availability for use of works for nonprofit archival, preservation, and educational purposes;

(iii) the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research;

(iv) the effect of circumvention of technological measures on the market for or value of copyrighted works; and

(v) such other factors as the Librarian considers appropriate.

(D) The Librarian shall publish any class of copyrighted works for which the Librarian has determined, pursuant to the rulemaking conducted under subparagraph (C), that noninfringing uses by persons who are users of a copyrighted work are, or are likely to be, adversely affected, and the prohibition contained in subparagraph (A) shall not apply to such users with respect to such class of works for the ensuing 3-year period.

(E) Neither the exception under subparagraph (B) from the applicability of the prohibition contained in subparagraph (A), nor any determination made in a rulemaking conducted under subparagraph (C), may be used as a defense in any action to enforce any provision of this title other than this paragraph.

(2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that –

(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;

(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

(3) As used in this subsection –

(A) to "circumvent a technological measure" means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner; and

Appendix C

(B) a technological measure "effectively controls access to a work" if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work.

(b) Additional violations. - (1) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that –

(A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof;

(B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.

Appendix C

(2) As used in this subsection –

(A) to "circumvent protection afforded by a technological measure" means avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure; and

(B) a technological measure "effectively protects a right of a copyright owner under this title" if the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title.

(c) Other rights, etc., not affected. - (1) Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title.

(2) Nothing in this section shall enlarge or diminish vicarious or contributory liability for copyright infringement in connection with any technology, product, service, device, component, or part thereof.

(3) Nothing in this section shall require that the design of, or design and selection of parts and components for, a consumer electronics, telecommunications, or computing product provide for a response to any particular technological measure, so long as such part or component, or the product in which such part or component is integrated, does not otherwise fall within the prohibitions of subsection (a)(2) or (b)(1).

Appendix C

(4) Nothing in this section shall enlarge or diminish any rights of free speech or the press for activities using consumer electronics, telecommunications, or computing products.

(d) Exemption for nonprofit libraries, archives, and educational institutions. - (1) A nonprofit library, archives, or educational institution which gains access to a commercially exploited copyrighted work solely in order to make a good faith determination of whether to acquire a copy of that work for the sole purpose of engaging in conduct permitted under this title shall not be in violation of subsection (a)(1)(A). A copy of a work to which access has been gained under this paragraph –

(A) may not be retained longer than necessary to make such good faith determination; and

(B) may not be used for any other purpose.

(2) The exemption made available under paragraph (1) shall only apply with respect to a work when an identical copy of that work is not reasonably available in another form.

(3) A nonprofit library, archives, or educational institution that willfully for the purpose of commercial advantage or financial gain violates paragraph (1) –

(A) shall, for the first offense, be subject to the civil remedies under section 1203; and

(B) shall, for repeated or subsequent offenses, in addition to the civil remedies under section 1203, forfeit the exemption provided under paragraph (1).

(4) This subsection may not be used as a defense to a claim under subsection (a)(2) or (b), nor may this subsection permit a nonprofit library, archives, or educational institution to manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, component, or part thereof, which circumvents a technological measure.

(5) In order for a library or archives to qualify for the exemption under this subsection, the collections of that library or archives shall be –

(A) open to the public; or

(B) available not only to researchers affiliated with the library or archives or with the institution of which it is a part, but also to other persons doing research in a specialized field.

(e) Law enforcement, intelligence, and other government activities. - This section does not prohibit any lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent, or employee of the United States, a State, or a political subdivision of a State, or a person acting pursuant to a contract with the United States, a State, or a political subdivision of a State. For purposes of this subsection, the term ''information security'' means activities carried out in order to identify and address the vulnerabilities of a government computer, computer system, or computer network.

Appendix C

(f) Reverse engineering. - (1) Notwithstanding the provisions of subsection (a)(1)(A), a person who has lawfully obtained the right to use a copy of a computer program may circumvent a technological measure that effectively controls access to a particular portion of that program for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been readily available to the person engaging in the circumvention, to the extent any such acts of identification and analysis do not constitute infringement under this title.

(2) Notwithstanding the provisions of subsections (a)(2) and (b), a person may develop and employ technological means to circumvent a technological measure, or to circumvent protection afforded by a technological measure, in order to enable the identification and analysis under paragraph (1), or for the purpose of enabling interoperability of an independently created computer program with other programs, if such means are necessary to achieve such interoperability, to the extent that doing so does not constitute infringement under this title.

(3) The information acquired through the acts permitted under paragraph (1), and the means permitted under paragraph (2), may be made available to others if the person referred to in paragraph (1) or (2), as the case may be, provides such information or means solely for the purpose of enabling interoperability of an independently created computer program with other programs, and to the extent that doing so does not constitute infringement under this title or violate applicable law other than this section.

(4) For purposes of this subsection, the term "interoperability" means the ability of computer programs to exchange information, and of such programs mutually to use the information which has been exchanged.

(g) Encryption research. –

(1) Definitions. - For purposes of this subsection –

(A) the term "encryption research" means activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works, if these activities are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products; and

(B) the term "encryption technology" means the scrambling and descrambling of information using mathematical formulas or algorithms.

(2) Permissible acts of encryption research. - Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a technological measure as applied to a copy, phonorecord, performance, or display of a published work in the course of an act of good faith encryption research if –

(A) the person lawfully obtained the encrypted copy, phonorecord, performance, or display of the published work;

(B) such act is necessary to conduct such encryption research;

(C) the person made a good faith effort to obtain authorization before the circumvention; and

(D) such act does not constitute infringement under this title or a violation of applicable law other than this section, including section 1030 of title 18 and those provisions of title 18 amended by the Computer Fraud and Abuse Act of 1986.

(3) Factors in determining exemption. - In determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include –

(A) whether the information derived from the encryption research was disseminated, and if so, whether it was disseminated in a manner reasonably calculated to advance the state of knowledge or development of encryption technology, versus whether it was disseminated in a manner that facilitates infringement under this title or a violation of applicable law other than this section [17 U.S.C.A. §1 et seq.], including a violation of privacy or breach of security;

(B) whether the person is engaged in a legitimate course of study, is employed, or is appropriately trained or experienced, in the field of encryption technology; and

(C) whether the person provides the copyright owner of the work to which the technological measure is applied with notice of the findings and documentation of the research, and the time when such notice is provided.

Appendix C

(4) Use of technological means for research activities. - Notwithstanding the provisions of subsection (a)(2), it is not a violation of that subsection for a person to –

(A) develop and employ technological means to circumvent a technological measure for the sole purpose of that person performing the acts of good faith encryption research described in paragraph (2); and

(B) provide the technological means to another person with whom he or she is working collaboratively for the purpose of conducting the acts of good faith encryption research described in paragraph (2) or for the purpose of having that other person verify his or her acts of good faith encryption research described in paragraph (2).

(5) Report to Congress. - Not later than 1 year after the date of the enactment of this chapter [17 U.S.C.A. §1 et seq.],, the Register of Copyrights and the Assistant Secretary for Communications and Information of the Department of Commerce shall jointly report to the Congress on the effect this subsection has had on –

(A) encryption research and the development of encryption technology;

(B) the adequacy and effectiveness of technological measures designed to protect copyrighted works; and

(C) protection of copyright owners against the unauthorized access to their encrypted copyrighted works.

The report shall include legislative recommendations, if any.

Appendix C

(h) Exceptions regarding minors. - In applying subsection (a) to a component or part, the court may consider the necessity for its intended and actual incorporation in a technology, product, service, or device, which –

(1) does not itself violate the provisions of this title; and

(2) has the sole purpose to prevent the access of minors to material on the Internet.

(i) Protection of personally identifying information. –

(1) Circumvention permitted. - Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a technological measure that effectively controls access to a work protected under this title, if –

(A) the technological measure, or the work it protects, contains the capability of collecting or disseminating personally identifying information reflecting the online activities of a natural person who seeks to gain access to the work protected;

(B) in the normal course of its operation, the technological measure, or the work it protects, collects or disseminates personally identifying information about the person who seeks to gain access to the work protected, without providing conspicuous notice of such collection or dissemination to such person, and without providing such person with the capability to prevent or restrict such collection or dissemination;

Appendix C

(C) the act of circumvention has the sole effect of identifying and disabling the capability described in subparagraph (A), and has no other effect on the ability of any person to gain access to any work; and

(D) the act of circumvention is carried out solely for the purpose of preventing the collection or dissemination of personally identifying information about a natural person who seeks to gain access to the work protected, and is not in violation of any other law.

(2) Inapplicability to certain technological measures. - This subsection does not apply to a technological measure, or a work it protects, that does not collect or disseminate personally identifying information and that is disclosed to a user as not having or using such capability.

(j) Security Testing. –

(1) Definition. - For purposes of this subsection, the term "security testing" means accessing a computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability, with the authorization of the owner or operator of such computer, computer system, or computer network.

(2) Permissible acts of security testing. - Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to engage in an act of security testing, if such act does not constitute infringement under this title or a violation of applicable law other than this section, including section 1030 of title 18 and those provisions of title 18 amended by the Computer Fraud and Abuse Act of 1986.

Appendix C

(3) Factors in determining exemption. - In determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include –

(A) whether the information derived from the security testing was used solely to promote the security of the owner or operator of such computer, computer system or computer network, or shared directly with the developer of such computer, computer system, or computer network; and

(B) whether the information derived from the security testing was used or maintained in a manner that does not facilitate infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security.

(4) Use of technological means for security testing. - Notwithstanding the provisions of subsection (a)(2), it is not a violation of that subsection for a person to develop, produce, distribute or employ technological means for the sole purpose of performing the acts of security testing described in subsection (2),[1] provided such technological means does not otherwise violate section[2] (a)(2).

(k) Certain analog devices and certain technological measures. –

(1) Certain analog devices. –

(A) Effective 18 months after the date of the enactment of this chapter, no person shall manufacture, import, offer to the public, provide or otherwise traffic in any –

---

1. So in original. Probably should be "subsection (a)(2)".

2. So in original. Probably should be "subsection".

Appendix C

(i) VHS format analog video cassette recorder unless such recorder conforms to the automatic gain control copy control technology;

(ii) 8mm format analog video cassette camcorder unless such camcorder conforms to the automatic gain control technology;

(iii) Beta format analog video cassette recorder, unless such recorder conforms to the automatic gain control copy control technology, except that this requirement shall not apply until there are 1,000 Beta format analog video cassette recorders sold in the United States in any one calendar year after the date of the enactment of this chapter;

(iv) 8mm format analog video cassette recorder that is not an analog video cassette camcorder, unless such recorder conforms to the automatic gain control copy control technology, except that this requirement shall not apply until there are 20,000 such recorders sold in the United States in any one calendar year after the date of the enactment of this chapter; or

(v) analog video cassette recorder that records using an NTSC format video input and that is not otherwise covered under clauses (i) through (iv), unless such device conforms to the automatic gain control copy control technology.

Appendix C

(B) Effective on the date of the enactment of this chapter, no person shall manufacture, import, offer to the public, provide or otherwise traffic in –

(i) any VHS format analog video cassette recorder or any 8mm format analog video cassette recorder if the design of the model of such recorder has been modified after such date of enactment so that a model of recorder that previously conformed to the automatic gain control copy control technology no longer conforms to such technology; or

(ii) any VHS format analog video cassette recorder, or any 8mm format analog video cassette recorder that is not an 8mm analog video cassette camcorder, if the design of the model of such recorder has been modified after such date of enactment so that a model of recorder that previously conformed to the four-line colorstripe copy control technology no longer conforms to such technology.

Manufacturers that have not previously manufactured or sold a VHS format analog video cassette recorder, or an 8mm format analog cassette recorder, shall be required to conform to the four-line colorstripe copy control technology in the initial model of any such recorder manufactured after the date of the enactment of this chapter, and thereafter to continue conforming to the four-line colorstripe copy control technology. For purposes of this subparagraph, an analog video cassette recorder ''conforms to'' the four-line colorstripe copy control technology if it records a signal that, when played back by the playback function of that recorder in the normal viewing mode, exhibits, on a reference display device, a display containing distracting visible lines through portions of the viewable picture.

Appendix C

(2) Certain encoding restrictions. - No person shall apply the automatic gain control copy control technology or colorstripe copy control technology to prevent or limit consumer copying except such copying –

(A) of a single transmission, or specified group of transmissions, of live events or of audiovisual works for which a member of the public has exercised choice in selecting the transmissions, including the content of the transmissions or the time of receipt of such transmissions, or both, and as to which such member is charged a separate fee for each such transmission or specified group of transmissions;

(B) from a copy of a transmission of a live event or an audiovisual work if such transmission is provided by a channel or service where payment is made by a member of the public for such channel or service in the form of a subscription fee that entitles the member of the public to receive all of the programming contained in such channel or service;

(C) from a physical medium containing one or more prerecorded audiovisual works; or

(D) from a copy of a transmission described in subparagraph (A) or from a copy made from a physical medium described in subparagraph (C).

In the event that a transmission meets both the conditions set forth in subparagraph (A) and those set forth in subparagraph (B), the transmission shall be treated as a transmission described in subparagraph (A).

Appendix C

(3) Inapplicability. - This subsection shall not –

(A) require any analog video cassette camcorder to conform to the automatic gain control copy control technology with respect to any video signal received through a camera lens;

(B) apply to the manufacture, importation, offer for sale, provision of, or other trafficking in, any professional analog video cassette recorder; or

(C) apply to the offer for sale or provision of, or other trafficking in, any previously owned analog video cassette recorder, if such recorder was legally manufactured and sold when new and not subsequently modified in violation of paragraph (1)(B).

(4) Definitions. - For purposes of this subsection:

(A) An "analog video cassette recorder" means a device that records, or a device that includes a function that records, on electromagnetic tape in an analog format the electronic impulses produced by the video and audio portions of a television program, motion picture, or other form of audiovisual work.

(B) An "analog video cassette camcorder" means an analog video cassette recorder that contains a recording function that operates through a camera lens and through a video input that may be connected with a television or other video playback device.

Appendix C

(C) An analog video cassette recorder ''conforms'' to the automatic gain control copy control technology if it –

(i) detects one or more of the elements of such technology and does not record the motion picture or transmission protected by such technology; or

(ii) records a signal that, when played back, exhibits a meaningfully distorted or degraded display.

(D) The term "professional analog video cassette recorder" means an analog video cassette recorder that is designed, manufactured, marketed, and intended for use by a person who regularly employs such a device for a lawful business or industrial use, including making, performing, displaying, distributing, or transmitting copies of motion pictures on a commercial scale.

(E) The terms "VHS format", "8mm format", "Beta format", "automatic gain control copy control technology", "colorstripe copy control technology", "four-line version of the colorstripe copy control technology", and "NTSC" have the meanings that are commonly understood in the consumer electronics and motion picture industries as of the date of the enactment of this chapter.

(5) Violations. - Any violation of paragraph (1) of this subsection shall be treated as a violation of subsection (b)(1) of this section. Any violation of paragraph (2) of this subsection shall be deemed an ''act of circumvention'' for the purposes of section 1203(c)(3)(A) of this chapter.

Appendix C

Section 1202. Integrity of copyright management information

(a) False Copyright Management Information. - No person shall knowingly and with the intent to induce, enable, facilitate, or conceal infringement –

(1) provide copyright management information that is false, or

(2) distribute or import for distribution copyright management information that is false.

(b) Removal or Alteration of Copyright Management Information. - No person shall, without the authority of the copyright owner or the law –

(1) intentionally remove or alter any copyright management information,

(2) distribute or import for distribution copyright management information knowing that the copyright management information has been removed or altered without authority of the copyright owner or the law, or

(3) distribute, import for distribution, or publicly perform works, copies of works, or phonorecords, knowing that copyright management information has been removed or altered without authority of the copyright owner or the law,

knowing, or, with respect to civil remedies under section 1203, having reasonable grounds to know, that it will induce, enable, facilitate, or conceal an infringement of any right under this title.

(c) Definition. - As used in this section, the term ''copyright management information'' means any of the following information conveyed in connection with copies or phonorecords of a work or performances or displays of a work, including in digital form, except that such term does not include any personally identifying information about a user of a work or of a copy, phonorecord, performance, or display of a work:

(1) The title and other information identifying the work, including the information set forth on a notice of copyright.

(2) The name of, and other identifying information about, the author of a work.

(3) The name of, and other identifying information about, the copyright owner of the work, including the information set forth in a notice of copyright.

(4) With the exception of public performances of works by radio and television broadcast stations, the name of, and other identifying information about, a performer whose performance is fixed in a work other than an audiovisual work.

(5) With the exception of public performances of works by radio and television broadcast stations, in the case of an audiovisual work, the name of, and other identifying information about, a writer, performer, or director who is credited in the audiovisual work.

(6) Terms and conditions for use of the work.

(7) Identifying numbers or symbols referring to such information or links to such information.

(8) Such other information as the Register of Copyrights may prescribe by regulation, except that the Register of Copyrights may not require the provision of any information concerning the user of a copyrighted work.

(d) Law Enforcement, Intelligence, and Other Government Activities. - This section does not prohibit any lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent, or employee of the United States, a State, or a political subdivision of a State, or a person acting pursuant to a contract with the United States, a State, or a political subdivision of a State. For purposes of this subsection, the term ''information security'' means activities carried out in order to identify and address the vulnerabilities of a government computer, computer system, or computer network.

(e) Limitations on Liability. –

(1) Analog transmissions. - In the case of an analog transmission, a person who is making transmissions in its capacity as a broadcast station, or as a cable system, or someone who provides programming to such station or system, shall not be liable for a violation of subsection (b) if –

(A) avoiding the activity that constitutes such violation is not technically feasible or would create an undue financial hardship on such person; and

(B) such person did not intend, by engaging in such activity, to induce, enable, facilitate, or conceal infringement of a right under this title.

(2) Digital transmissions. –

(A) If a digital transmission standard for the placement of copyright management information for a category of works is set in a voluntary, consensus standard-setting process involving a representative cross-section of broadcast stations or cable systems and copyright owners of a category of works that are intended for public performance by such stations or systems, a person identified in paragraph (1) shall not be liable for a violation of subsection (b) with respect to the particular copyright management information addressed by such standard if –

(i) the placement of such information by someone other than such person is not in accordance with such standard; and

(ii) the activity that constitutes such violation is not intended to induce, enable, facilitate, or conceal infringement of a right under this title.

(B) Until a digital transmission standard has been set pursuant to subparagraph (A) with respect to the placement of copyright management information for a category of works, a person identified in paragraph (1) shall not be liable for a violation of subsection (b) with respect to such copyright management information, if the activity that constitutes such violation is not intended to induce, enable, facilitate, or conceal infringement of a right under this title, and if –

(i) the transmission of such information by such person would result in a perceptible visual or aural degradation of the digital signal; or

(ii) the transmission of such information by such person would conflict with –

(I) an applicable government regulation relating to transmission of information in a digital signal;

(II) an applicable industry-wide standard relating to the transmission of information in a digital signal that was adopted by a voluntary consensus standards body prior to the effective date of this chapter; or

(III) an applicable industry-wide standard relating to the transmission of information in a digital signal that was adopted in a voluntary, consensus standards-setting process open to participation by a representative cross-section of broadcast stations or cable systems and copyright owners of a category of works that are intended for public performance by such stations or systems.

(3) Definitions. - As used in this subsection –

(A) the term ''broadcast station'' has the meaning given that term in section 3 of the Communications Act of 1934 (47 U.S.C. 153); and

(B) the term ''cable system'' has the meaning given that term in section 602 of the Communications Act of 1934 (47 U.S.C. 522).

Appendix C

Section 1203. Civil remedies

(a) Civil Actions. - Any person injured by a violation of section 1201 or 1202 may bring a civil action in an appropriate United States district court for such violation.

(b) Powers of the Court. - In an action brought under subsection (a), the court –

(1) may grant temporary and permanent injunctions on such terms as it deems reasonable to prevent or restrain a violation, but in no event shall impose a prior restraint on free speech or the press protected under the 1st amendment to the Constitution;

(2) at any time while an action is pending, may order the impounding, on such terms as it deems reasonable, of any device or product that is in the custody or control of the alleged violator and that the court has reasonable cause to believe was involved in a violation;

(3) may award damages under subsection (c);

(4) in its discretion may allow the recovery of costs by or against any party other than the United States or an officer thereof;

(5) in its discretion may award reasonable attorney's fees to the prevailing party; and

(6) may, as part of a final judgment or decree finding a violation, order the remedial modification or the destruction

of any device or product involved in the violation that is in the custody or control of the violator or has been impounded under paragraph (2).

(c) Award of Damages. –

(1) In general. - Except as otherwise provided in this title, a person committing a violation of section 1201 or 1202 is liable for either –

(A) the actual damages and any additional profits of the violator, as provided in paragraph (2), or

(B) statutory damages, as provided in paragraph (3).

(2) Actual damages. - The court shall award to the complaining party the actual damages suffered by the party as a result of the violation, and any profits of the violator that are attributable to the violation and are not taken into account in computing the actual damages, if the complaining party elects such damages at any time before final judgment is entered.

(3) Statutory damages. - (A) At any time before final judgment is entered, a complaining party may elect to recover an award of statutory damages for each violation of section 1201 in the sum of not less than $200 or more than $2,500 per act of circumvention, device, product, component, offer, or performance of service, as the court considers just.

(B) At any time before final judgment is entered, a complaining party may elect to recover an award of statutory damages for each violation of section 1202 in the sum of not less than $2,500 or more than $25,000.

Appendix C

(4) Repeated violations. - In any case in which the injured party sustains the burden of proving, and the court finds, that a person has violated section 1201 or 1202 within 3 years after a final judgment was entered against the person for another such violation, the court may increase the award of damages up to triple the amount that would otherwise be awarded, as the court considers just.

(5) Innocent violations. –

(A) In general. - The court in its discretion may reduce or remit the total award of damages in any case in which the violator sustains the burden of proving, and the court finds, that the violator was not aware and had no reason to believe that its acts constituted a violation.

(B) Nonprofit library, archives, educational institutions, or public broadcasting entities. –

(i) Definition. - In this subparagraph, the term "public broadcasting entity" has the meaning given such term under section 118(g).

(ii) In general. - In the case of a nonprofit library, archives, educational institution, or public broadcasting entity, the court shall remit damages in any case in which the library, archives, educational institution, or public broadcasting entity sustains the burden of proving, and the court finds, that the library, archives, educational institution, or public broadcasting entity was not aware and had no reason to believe that its acts constituted a violation.

Appendix C

Section 1204. Criminal offenses and penalties

(a) In General. - Any person who violates section 1201 or 1202 willfully and for purposes of commercial advantage or private financial gain –

(1) shall be fined not more than $500,000 or imprisoned for not more than 5 years, or both, for the first offense; and

(2) shall be fined not more than $1,000,000 or imprisoned for not more than 10 years, or both, for any subsequent offense.

(b) Limitation for Nonprofit Library, Archives, Educational Institution, or Public Broadcasting Entity. - Subsection (a) shall not apply to a nonprofit library, archives, educational institution, or public broadcasting entity (as defined under section 118(g).

(c) Statute of Limitations. - No criminal proceeding shall be brought under this section unless such proceeding is commenced within 5 years after the cause of action arose.

Appendix C

Section 1205. Savings clause

Nothing in this chapter abrogates, diminishes, or weakens the provisions of, nor provides any defense or element of mitigation in a criminal prosecution or civil action under, any Federal or State law that prevents the violation of the privacy of an individual in connection with the individual's use of the Internet.

APPENDIX D

TITLE II OF THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998, AS CODIFIED AT 17 U.S.C. § 512

Section 512. Limitations on liability relating to material online

(a) Transitory digital network communications. - A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if –

(1) the transmission of the material was initiated by or at the direction of a person other than the service provider;

(2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;

(3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;

(4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no

such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and

(5) the material is transmitted through the system or network without modification of its content.

(b) System caching. –

(1) Limitation on liability. - A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider in a case in which –

(A) the material is made available online by a person other than the service provider;

(B) the material is transmitted from the person described in subparagraph (A) through the system or network to a person other than the person described in subparagraph (A) at the direction of that other person; and

(C) the storage is carried out through an automatic technical process for the purpose of making the material available to users of the system or network who, after the material is transmitted as described in subparagraph (B), request access to the material from the person described in subparagraph (A), if the conditions set forth in paragraph (2) are met.

Appendix D

(2) Conditions. - The conditions referred to in paragraph (1) are that –

(A) the material described in paragraph (1) is transmitted to the subsequent users described in paragraph (1)(C) without modification to its content from the manner in which the material was transmitted from the person described in paragraph (1)(A);

(B) the service provider described in paragraph (1) complies with rules concerning the refreshing, reloading, or other updating of the material when specified by the person making the material available online in accordance with a generally accepted industry standard data communications protocol for the system or network through which that person makes the material available, except that this subparagraph applies only if those rules are not used by the person described in paragraph (1)(A) to prevent or unreasonably impair the intermediate storage to which this subsection applies;

(C) the service provider does not interfere with the ability of technology associated with the material to return to the person described in paragraph (1)(A) the information that would have been available to that person if the material had been obtained by the subsequent users described in paragraph (1)(C) directly from that person, except that this subparagraph applies only if that technology –

(i) does not significantly interfere with the performance of the provider's system or network or with the intermediate storage of the material;

(ii) is consistent with generally accepted industry standard communications protocols; and

(iii) does not extract information from the provider's system or network other than the information that would have been available to the person described in paragraph (1)(A) if the subsequent users had gained access to the material directly from that person;

(D) if the person described in paragraph (1)(A) has in effect a condition that a person must meet prior to having access to the material, such as a condition based on payment of a fee or provision of a password or other information, the service provider permits access to the stored material in significant part only to users of its system or network that have met those conditions and only in accordance with those conditions; and

(E) if the person described in paragraph (1)(A) makes that material available online without the authorization of the copyright owner of the material, the service provider responds expeditiously to remove, or disable access to, the material that is claimed to be infringing upon notification of claimed infringement as described in subsection (c)(3), except that this subparagraph applies only if –

(i) the material has previously been removed from the originating site or access to it has been disabled, or a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled; and

(ii) the party giving the notification includes in the notification a statement confirming that the material has been removed from the originating site or access to it has been disabled or that a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled.

(c) Information residing on systems or networks at direction of Users. –

(1) In general. - A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider –

(A)(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;

(ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

(iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

Appendix D

(C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.

(2) Designated agent. - The limitations on liability established in this subsection apply to a service provider only if the service provider has designated an agent to receive notifications of claimed infringement described in paragraph (3), by making available through its service, including on its website in a location accessible to the public, and by providing to the Copyright Office, substantially the following information:

(A) the name, address, phone number, and electronic mail address of the agent.

(B) other contact information which the Register of Copyrights may deem appropriate.

The Register of Copyrights shall maintain a current directory of agents available to the public for inspection, including through the Internet, in both electronic and hard copy formats, and may require payment of a fee by service providers to cover the costs of maintaining the directory.

(3) Elements of notification. –

(A) To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes substantially the following:

Appendix D

(i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

(ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.

(iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.

(iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.

(v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.

(vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

Appendix D

(B)(i) Subject to clause (ii), a notification from a copyright owner or from a person authorized to act on behalf of the copyright owner that fails to comply substantially with the provisions of subparagraph (A) shall not be considered under paragraph (1)(A) in determining whether a service provider has actual knowledge or is aware of facts or circumstances from which infringing activity is apparent.

(ii) In a case in which the notification that is provided to the service provider's designated agent fails to comply substantially with all the provisions of subparagraph (A) but substantially complies with clauses (ii), (iii), and (iv) of subparagraph (A), clause (i) of this subparagraph applies only if the service provider promptly attempts to contact the person making the notification or takes other reasonable steps to assist in the receipt of notification that substantially complies with all the provisions of subparagraph (A).

(d) Information location tools. - A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link, if the service provider –

(1)(A) does not have actual knowledge that the material or activity is infringing;

(B) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

(C) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(2) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

(3) upon notification of claimed infringement as described in subsection (c)(3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity, except that, for purposes of this paragraph, the information described in subsection (c)(3)(A)(iii) shall be identification of the reference or link, to material or activity claimed to be infringing, that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate that reference or link.

(e) Limitation on liability of nonprofit educational institutions. - (1) When a public or other nonprofit institution of higher education is a service provider, and when a faculty member or graduate student who is an employee of such institution is performing a teaching or research function, for the purposes of subsections (a) and (b) such faculty member or graduate student shall be considered to be a person other than the institution, and for the purposes of subsections (c) and (d) such faculty member's or graduate student's knowledge or awareness of his or her infringing activities shall not be attributed to the institution, if –

(A) such faculty member's or graduate student's infringing activities do not involve the provision of online

access to instructional materials that are or were required or recommended, within the preceding 3-year period, for a course taught at the institution by such faculty member or graduate student;

(B) the institution has not, within the preceding 3-year period, received more than two notifications described in subsection (c)(3) of claimed infringement by such faculty member or graduate student, and such notifications of claimed infringement were not actionable under subsection (f); and

(C) the institution provides to all users of its system or network informational materials that accurately describe, and promote compliance with, the laws of the United States relating to copyright.

(2) For the purposes of this subsection, the limitations on injunctive relief contained in subsections (j)(2) and (j)(3), but not those in (j)(1), shall apply.

(f) Misrepresentations. - Any person who knowingly materially misrepresents under this section –

(1) that material or activity is infringing, or

(2) that material or activity was removed or disabled by mistake or misidentification, shall be liable for any damages, including costs and attorneys' fees, incurred by the alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service

provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it.

(g) Replacement of removed or disabled material and limitation on other liability. –

(1) No liability for taking down generally. - Subject to paragraph (2), a service provider shall not be liable to any person for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringing.

(2) Exception. - Paragraph (1) shall not apply with respect to material residing at the direction of a subscriber of the service provider on a system or network controlled or operated by or for the service provider that is removed, or to which access is disabled by the service provider, pursuant to a notice provided under subsection (c)(1)(C), unless the service provider –

(A) takes reasonable steps promptly to notify the subscriber that it has removed or disabled access to the material;

(B) upon receipt of a counter notification described in paragraph (3), promptly provides the person who provided the notification under subsection (c)(1)(C) with a copy of

the counter notification, and informs that person that it will replace the removed material or cease disabling access to it in 10 business days; and

(C) replaces the removed material and ceases disabling access to it not less than 10, nor more than 14, business days following receipt of the counter notice, unless its designated agent first receives notice from the person who submitted the notification under subsection (c)(1)(C) that such person has filed an action seeking a court order to restrain the subscriber from engaging in infringing activity relating to the material on the service provider's system or network.

(3) Contents of counter notification. - To be effective under this subsection, a counter notification must be a written communication provided to the service provider's designated agent that includes substantially the following:

(A) A physical or electronic signature of the subscriber.

(B) Identification of the material that has been removed or to which access has been disabled and the location at which the material appeared before it was removed or access to it was disabled.

(C) A statement under penalty of perjury that the subscriber has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material to be removed or disabled.

(D) The subscriber's name, address, and telephone number, and a statement that the subscriber consents to the

jurisdiction of Federal District Court for the judicial district in which the address is located, or if the subscriber's address is outside of the United States, for any judicial district in which the service provider may be found, and that the subscriber will accept service of process from the person who provided notification under subsection (c)(1)(C) or an agent of such person.

(4) Limitation on other liability. - A service provider's compliance with paragraph (2) shall not subject the service provider to liability for copyright infringement with respect to the material identified in the notice provided under subsection (c)(1)(C).

(h) Subpoena To Identify Infringer. –

(1) Request. - A copyright owner or a person authorized to act on the owner's behalf may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer in accordance with this subsection.

(2) Contents of request. - The request may be made by filing with the clerk –

(A) a copy of a notification described in subsection (c)(3)(A);

(B) a proposed subpoena; and

(C) a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of

an alleged infringer and that such information will only be used for the purpose of protecting rights under this title.

(3) Contents of subpoena. - The subpoena shall authorize and order the service provider receiving the notification and the subpoena to expeditiously disclose to the copyright owner or person authorized by the copyright owner information sufficient to identify the alleged infringer of the material described in the notification to the extent such information is available to the service provider.

(4) Basis for granting subpoena. - If the notification filed satisfies the provisions of subsection (c)(3)(A), the proposed subpoena is in proper form, and the accompanying declaration is properly executed, the clerk shall expeditiously issue and sign the proposed subpoena and return it to the requester for delivery to the service provider.

(5) Actions of service provider receiving subpoena. - Upon receipt of the issued subpoena, either accompanying or subsequent to the receipt of a notification described in subsection (c)(3)(A), the service provider shall expeditiously disclose to the copyright owner or person authorized by the copyright owner the information required by the subpoena, notwithstanding any other provision of law and regardless of whether the service provider responds to the notification.

(6) Rules applicable to subpoena. - Unless otherwise provided by this section or by applicable rules of the court, the procedure for issuance and delivery of the subpoena, and the remedies for noncompliance with the subpoena, shall be governed to the greatest extent practicable by those provisions

of the Federal Rules of Civil Procedure governing the issuance, service, and enforcement of a subpoena duces tecum.

(i) Conditions for eligibility. –

(1) Accommodation of technology. - The limitations on liability established by this section shall apply to a service provider only if the service provider –

(A) has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers; and

(B) accommodates and does not interfere with standard technical measures.

(2) Definition. - As used in this subsection, the term "standard technical measures" means technical measures that are used by copyright owners to identify or protect copyrighted works and –

(A) have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process;

(B) are available to any person on reasonable and nondiscriminatory terms; and

(C) do not impose substantial costs on service providers or substantial burdens on their systems or networks.

(j) Injunctions. - The following rules shall apply in the case of any application for an injunction under section 502 against a service provider that is not subject to monetary remedies under this section:

(1) Scope of relief. - (A) With respect to conduct other than that which qualifies for the limitation on remedies set forth in subsection (a), the court may grant injunctive relief with respect to a service provider only in one or more of the following forms:

(i) An order restraining the service provider from providing access to infringing material or activity residing at a particular online site on the provider's system or network.

(ii) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is engaging in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.

(iii) Such other injunctive relief as the court may consider necessary to prevent or restrain infringement of copyrighted material specified in the order of the court at a particular online location, if such relief is the least burdensome to the service provider among the forms of relief comparably effective for that purpose.

(B) If the service provider qualifies for the limitation on remedies described in subsection (a), the court may only grant injunctive relief in one or both of the following forms:

(i) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is using the provider's service to engage in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.

(ii) An order restraining the service provider from providing access, by taking reasonable steps specified in the order to block access, to a specific, identified, online location outside the United States.

(2) Considerations. - The court, in considering the relevant criteria for injunctive relief under applicable law, shall consider –

(A) whether such an injunction, either alone or in combination with other such injunctions issued against the same service provider under this subsection, would significantly burden either the provider or the operation of the provider's system or network;

(B) the magnitude of the harm likely to be suffered by the copyright owner in the digital network environment if steps are not taken to prevent or restrain the infringement;

(C) whether implementation of such an injunction would be technically feasible and effective, and would not interfere with access to noninfringing material at other online locations; and

(D) whether other less burdensome and comparably effective means of preventing or restraining access to the infringing material are available.

(3) Notice and ex parte orders. - Injunctive relief under this subsection shall be available only after notice to the service provider and an opportunity for the service provider to appear are provided, except for orders ensuring the preservation of evidence or other orders having no material adverse effect on the operation of the service provider's communications network.

(k) Definitions. –

(1) Service provider. - (A) As used in subsection (a), the term "service provider" means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.

(B) As used in this section, other than subsection (a), the term "service provider" means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A).

Appendix D

(2) Monetary relief. - As used in this section, the term "monetary relief" means damages, costs, attorneys' fees, and any other form of monetary payment.

(l) Other defenses not affected. - The failure of a service provider's conduct to qualify for limitation of liability under this section shall not bear adversely upon the consideration of a defense by the service provider that the service provider's conduct is not infringing under this title or any other defense.

(m) Protection of privacy. - Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) on –

(1) a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i); or

(2) a service provider gaining access to, removing, or disabling access to material in cases in which such conduct is prohibited by law.

(n) Construction. - Subsections (a), (b), (c), and (d) describe separate and distinct functions for purposes of applying this section. Whether a service provider qualifies for the limitation on liability in any one of those subsections shall be based solely on the criteria in that subsection, and shall not affect a determination of whether that service provider qualifies for the limitations on liability under any other such subsection.